control²

User Guide

BX600 Digital KVM Switch

Keyboard/Video/Mouse Switch English

FUJITSU COMPUTERS SIEMENS

USA Notification

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japanese Notification

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Notification

기종별	사용자 안내문
A급 기기 (업무용 정보통신기기)	이기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 구입 하였을 때에는 가정용으로 교환하시기 바랍니다.

BX600 Digital KVM Switch

Edition March 2008

Comments... Suggestions... Corrections

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs. Contact information is included in the back of the manual.

Certified documentation according to DIN EN ISO 9001:2000

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2000.

Copyright and Trademarks

Copyright © 2007 Fujitsu Siemens Computers GmbH.

All rights reserved.

Avocent, the Avocent logo and OSCAR graphical user interface are registered trademarks of Avocent Corporation or its affiliates.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

Contents

1	**Product Overview**	**1**
1.1	Features and Benefits	1
1.1.1	OSCAR Graphical User Interface	2
1.1.2	Network Connectivity	2
1.1.3	Control of Virtual Media	2
1.1.4	Security	2
1.1.5	Scanning	2
1.1.6	Identify Server Modules	2
1.1.7	Tiering	2
1.2	Notational Conventions	2
2	**Initial Browser Setup**	**5**
2.1	Installing the JRE for Windows Clients	5
2.2	Installing the JRE for Linux Clients	6
2.3	DKVM network configuration	7
2.3.1	Default IP address	7
2.3.2	IP address configuration	8
2.3.3	Network port settings	8
2.3.4	Internet Browser Security Settings	8
2.3.5	MMB and DKVM certificate integration into the IE6 browser's store of trust-	
ed sites		10
2.4	Avoiding Security Alerts when Launching the Viewer	17
2.4.1	Internet Explorer 7 on Windows Vista Client	17
2.4.2	Internet Explorer 6 on Windows Client	18
2.4.3	Mozilla Firefox 1.5 on Red Hat 4	23
2.4.4	Mozilla 1.7.12 on Red Hat 4	30
2.4.5	Mozilla 1.7.5 on SUSE9	36
2.5	Finding the dKVM IP-address when using DHCP	44
2.5.1	Integrating the DKVM IP address with https setting	45
2.5.2	Resolutions supported by the DKVM Console Viewer	45
3	**Installation**	**47**
3.1	Configuring the BX600 Digital KVM Switch	47
3.2	Setting Up a BX600 Digital KVM Switch in Tiers	48
3.2.1	Tiering a BX600 Digital KVM Switch from a Console Switch	50
4	**Analog Operation**	**53**
4.1	Controlling Your System	53
4.2	Viewing and Selecting Slots and Server Modules	53
4.2.0.1	Selecting Server Modules	54
4.2.0.2	Soft Switching	54

4.3	OSCAR Interface Navigation Basics	55
4.4	Configuring the OSCAR Interface	56
4.4.1	Assigning Server Module Names	57
4.4.2	Changing the Display Behavior	58
4.4.3	Controlling the Status Flag	59
4.4.4	Setting Console Security	60
4.5	Displaying Version Information	63
4.6	Scanning Your System	63
5	**Digital Operation**	**67**
5.1	Accessing BX600 Digital KVM Switch through Fujitsu Siemens (MMB)	67
5.2	Using the Video Viewer	68
5.2.1	Interacting With the Server Being Viewed	68
5.2.1.1	Server Name Modifications	68
5.2.1.2	Video Viewer command panel	70
5.2.1.3	KVM Session Premption	70
5.2.1.4	Current user response to preemption request	71
5.2.2	Viewer Window Features	73
5.2.3	Expanding and Refreshing Your Viewer	73
5.2.4	Adjusting the Viewer Window	74
5.2.5	Adjusting Keyboard Macros	74
5.2.6	Setting a Keystroke Prefix	74
5.2.7	Adjusting Mouse Acceleration	74
5.2.8	Adjusting the Video Quality	74
5.2.9	Manual Video Adjust Dialog Box Options	75
5.2.10	Minimizing Remote Video Session Discoloration	75
5.2.11	Improving Screen Background Color Display	76
5.2.12	Improving Mouse Performance	76
5.2.13	Create Screenshot Images	77
5.3	Virtual Media	77
5.3.1	Virtual Media Dialog Box	77
5.3.1.1	Mapping a Floppy Device	78
5.3.1.2	Mapping a CD/DVD Device	79
5.3.1.3	Viewing the Mapped Device Status	79
6	**BX600 Graphical User Interface**	**81**
6.1	DKVM Blade Folder Contents	81
6.2	Blade Info	81
6.3	Network Configuration	82
6.4	Console Redirection	83
6.5	Virtual Media	84
6.6	FW Update	84

7 Appendices 85
7.1 FAQs (Frequently Asked Questions) 85
7.2 Technical Specifications 89
7.3 Minimum Requirements for Video Viewer and Virtual Media Interface ... 89
7.4 OSCAR Interface Refresh Rates 90
7.5 Technical Support 91
7.5.1 Before you call 91

Contents

1 Product Overview

1.1 Features and Benefits

The Fujitsu Siemens BX600 Digital KVM Switch is integrated in your Fujitsu Siemens BX600 blade chassis. It allows you to manage many server modules through a single keyboard, monitor, and mouse. In addition, through virtual media, you can control your remote servers as if you were physically present.

You can also connect cables from the BX600 Digital KVM Switch to a KVM appliance such as the Fujitsu Siemens s3-1621 Console Switch. This capability allows you to create large combinations of servers and switches that you can manage from a common access point or over your IP network.

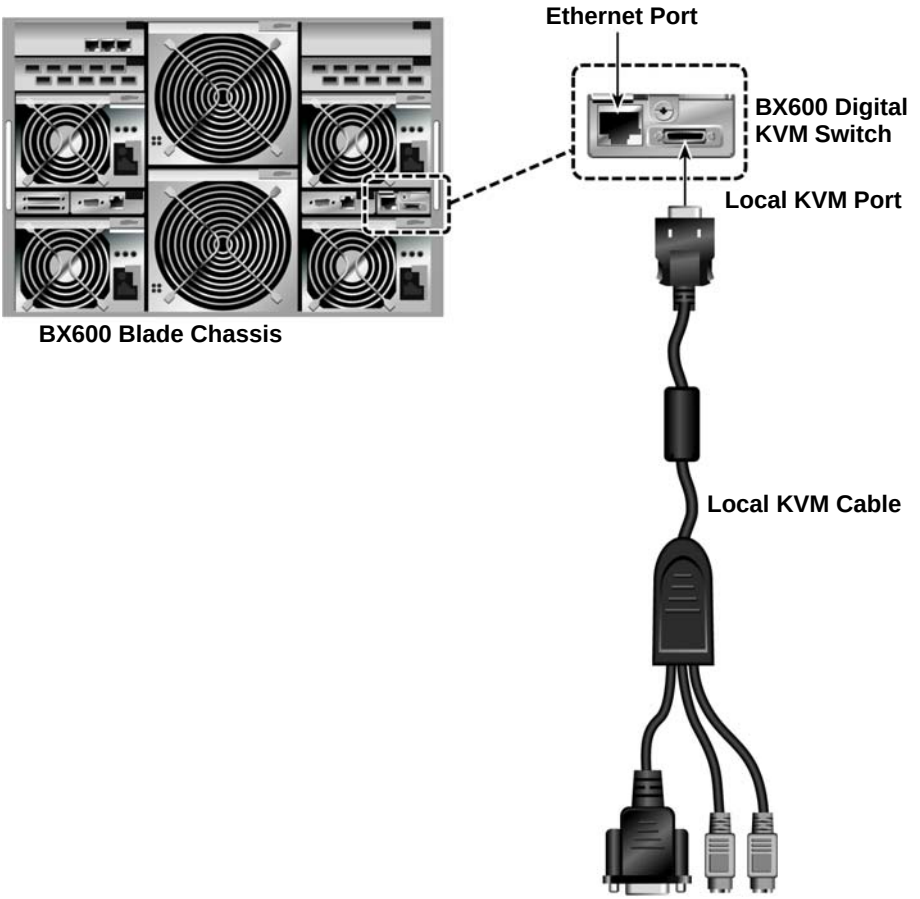

Figure 1: BX600 Digital KVM Switch

1.1.1 OSCAR Graphical User Interface

Select the server you would like and then manage it using the OSCAR® graphical user interface (On Screen Configuration and Activity Reporting). The OSCAR interface intuitive menus make managing your BX600 Digital KVM Switch system easy.

1.1.2 Network Connectivity

Using an ethernet connection, you can attach your BX600 Digital KVM Switch to your network, allowing you to control the blade servers and any attached virtual media appliances remotely.

1.1.3 Control of Virtual Media

The BX600 Digital KVM Switch allows you to view, move, or copy data from your client machine to any blade server. This feature enables you to manage remote systems by allowing you to install operating systems, recover hard drives, and back up servers, to name a few examples.

1.1.4 Security

The OSCAR interface allows you to protect your system with a screen saver password. After an amount of time that you define, the screen saver mode engages and access is prohibited until you enter the appropriate password to reactivate your system.

1.1.5 Scanning

When in Scan Mode, the OSCAR interface allows you to visually monitor server modules by displaying them one at a time, for the amount of time you specify.

1.1.6 Identify Server Modules

Through the OSCAR interface, you can easily assign names to server modules for your convenience. (By default all server modules are given the name Slot followed by the slot number.)

1.1.7 Tiering

The BX600 Digital KVM Switch can be set up in tiers from an existing Fujitsu Siemens KVM switch. The server modules can then be accessed through the software of the Fujitsu Siemens KVM switch.

1.2 Notational Conventions

The following notational conventions are used in this manual:

Bold	This indicates emphasis in the text.
Key	This indicates keys or key combinations in continuous text.
Italics	This indicates commands, file names, menu names and inputs in continuous text.

	This indicates additional information and tips.
Title	This indicates information, which if not heeded, may jeopardize your health, the functioning of your system or the security of your data.
▸	This indicates a step that you have to perform.
- and •	These characters symbolize itemized lists.
`Bold monospace font`	This indicates user inputs in examples.

2 Initial Browser Setup

The following browsers are supported for client machines managing the BX600 Server Blade Chassis:

- Internet Explorer 7.0 for Windows Vista Business
- Internet Explorer 6.0 (w/SP1, w/SP2) for Windows XP and Windows 2003
- Mozilla Firefox 1.5 for Red Hat 4 Linux
- Mozilla 1.7.12 for Red Hat 4 Linux
- Mozilla 1.7.5 for SuSE 9 Linux

The Management Module Board's (MMB) embedded web server has a web page for downloading two Java-based clients, the Java Viewer Client and the Java Virtual Media client. After the MMB authenticates the connection to the dKVM, the dKVM's embedded web server sends the appropriate Java client to the client's browser. Both Java application clients require a Java Runtime Environment (JRE) version 1.4.2 or greater. The JRE is a software bundle from Sun Microsystems that allows the client OS to run a Java application.

A released Java Runtime Environment version is available on the Fujitsu Siemens Computers ServerStart CD/DVD and the DKVM Support CD

2.1 Installing the JRE for Windows Clients

If the client OS is Windows, the JRE installation requires:

- the Windows Installer to be on your client machine

  -or-

- an active Internet connection is available in order for the JRE to be downloaded automatically.

When installing the JRE, the program InstallShield requires the Microsoft Windows Installer (version 2.0 or greater[1]) to be on your machine; if it is not found (or an older version is found), then InstallShield automatically tries to download Microsoft Windows Installer.

If your client machine is not on the Internet or is behind an authenticated proxy, the installation will fail at that point. To proceed, simply use the Windows Offline Installer from the Java download page at http://www.java.com/en/download simply follow the instructions presented by the Java download page.

A Microsoft Windows Installer (version 2.0 or greater) is included in this download.

Alternatively, you can manually download Microsoft Windows Installer by going to microsoft.com and searching for "Windows Installer".

To see which version of Microsoft Windows Installer is installed on your client:

- Locate the file MSI.DLL (usually located in C:\WINDOWS\SYSTEM32).
- Select the file and right-click on it.

1. Version 2.0 of Microsoft Windows Installer is included in Windows XP and Windows 2000 Service Pack 3. Version 3.1 of the Windows Installer is included in Windows 2003 SP1.

- Choose **Properties** and click on the **Version** tab.

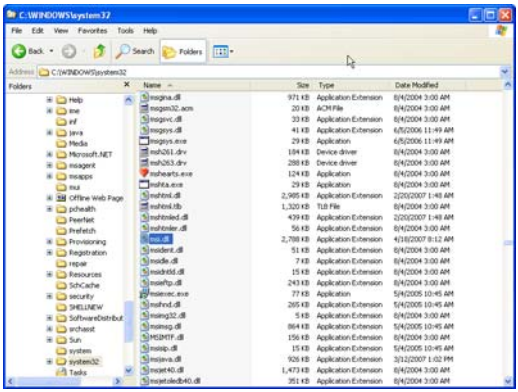

Figure 2: Locating MSI.DLL

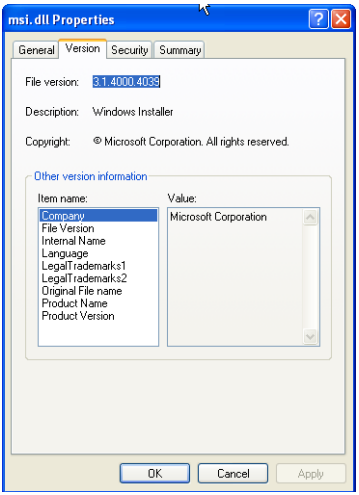

Figure 3: Viewing the MSI.DSL Version

2.2 Installing the JRE for Linux Clients

Go to http://www.java.com/en/download/linux_manual.jsp

There are two types of installation packages:

- Linux RPM package
- Linux self extracting binary file.

- Download the package that best suits your needs. Follow the instructions outlined on the web site.
- To test that the JRE is installed, enabled and working properly on your computer, run the test applet from the following web site:

  http://www.java.com/en/download/installed.jsp

2.3 DKVM network configuration

2.3.1 Default IP address

The Ethernet port on FSC-DRM is manually configurable from the (MMB) web pages. Configuration data is passed via the FSC BX600 chassis I2C bus.

The default IP address configuration is static. (DHCP is turned off by default)

- The default settings are:
  - **Hostname:** FSCDigitalKVM
  - **IP address:** 192.168.0.121
  - **Subnet mask:** 255.255.255.0
  - **Gateway IP address:** 192.168.0.1

The MMB default IP address is 192.168.0.120, but it is configurable by the user[1].

To launch the KVM configuration web page:

- To get to the MMB web page, point your browser to the IP address of the MMB.
- Once you have access to the MMB web page, mouse click on the **DKVM Blade** folder on the left of the page. The DKVM Blade folder expands
- Click on the **Network Configuration** link to launch the KVM Configuration page.

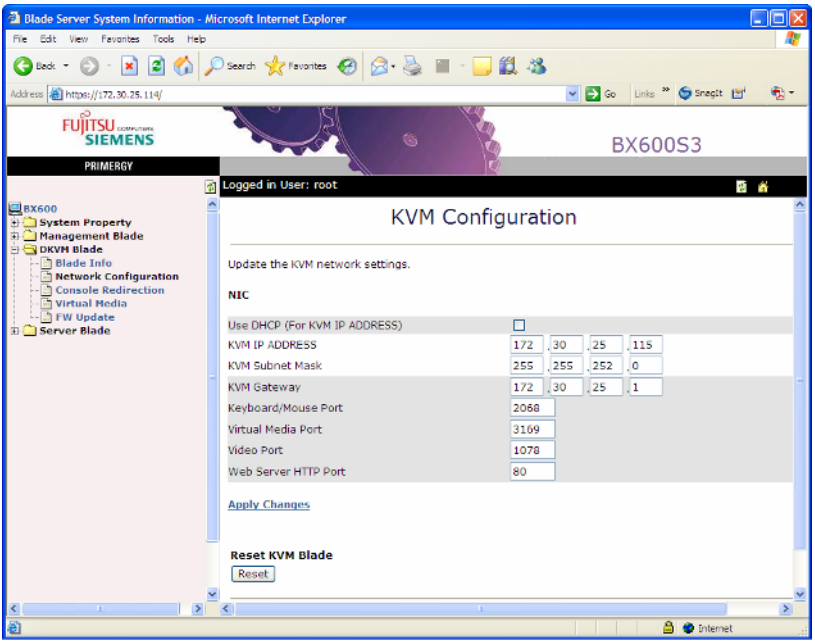

Figure 4: KVM Configuration Page

1. The IP address of the MMB and the IP address of the dKVM must be of the same subnet.

2.3.2 IP address configuration

Once you have access to the KVM Configuration page, if you want to use a static IP address, you can set the IP address of the KVM to any valid IP address you choose as long as that address is in the same subnet as that of the MMB.

If you want to use DHCP, then mouse click the box labeled **Use DHCP (For KVM IP Address)**

The given IP-Address will be shown after a few seconds by an update of the network configuration page.

2.3.3 Network port settings

The following ports can be configured from the KVM Configuration page:

- Keyboard/Mouse Port
- Virtual Media Port
- Video Port

Their respective defaults are 2068, 3169, 1078, and 80 but you can manually type in appropriate values in the fields for each port.

For example:

Keyboard/Mouse Port	: 2068	(2 ports are required)
Virtual Media Port	: 3169	
Video Port	: 1078	
Web Server HTTP port	: 80	

2.3.4 Internet Browser Security Settings

To configure the IE7 browser with recommended security settings:

- Click on the **Tools** menu of the IE7 menu list.
- Click on **Internet Options** of the Tools drop-down menu.

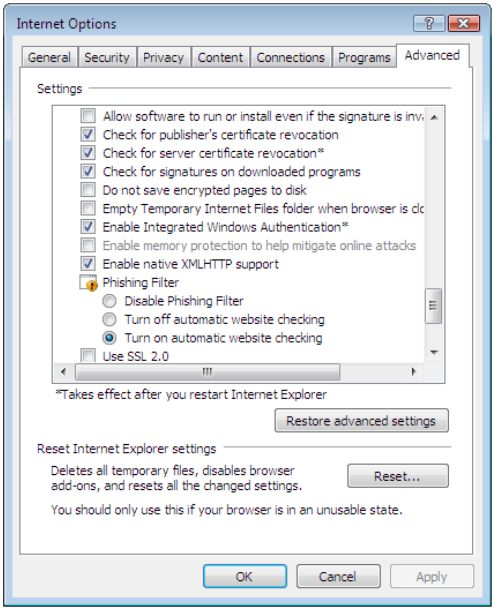
Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Allow software to run or install even if the signature is inv
Check for publisher's certificate revocation
Check for server certificate revocation*
Check for signatures on downloaded programs
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is cl
Enable Integrated Windows Authentication*
Enable memory protection to help mitigate online attacks
Enable native XMLHTTP support
Phishing Filter
Disable Phishing Filter
Turn off automatic website checking
Turn on automatic website checking
Use SSL 2.0
*Takes effect after you restart Internet Explorer
Restore advanced settings
Reset Internet Explorer settings
Deletes all temporary files, disables browser add-ons, and resets all the changed settings.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

Figure 5: Internet Explorer 7 Internet Options Advanced Dialog

- Click on the **Advanced** tab of the Internet Options dialog.
- Click on the button, **Reset...** to assure the Security settings are appropriate for accessing the FSC BX600 Server Blade Chassis.
- Make sure the box labeled, *Do not save encrypted pages to disk* is **not** checked.
- Click **OK**.

To configure the IE6 browser with recommended security settings:

- Click on the **Tools** menu of the IE6 menu list.
- Click on **Internet Options** of the Tools drop-down menu.

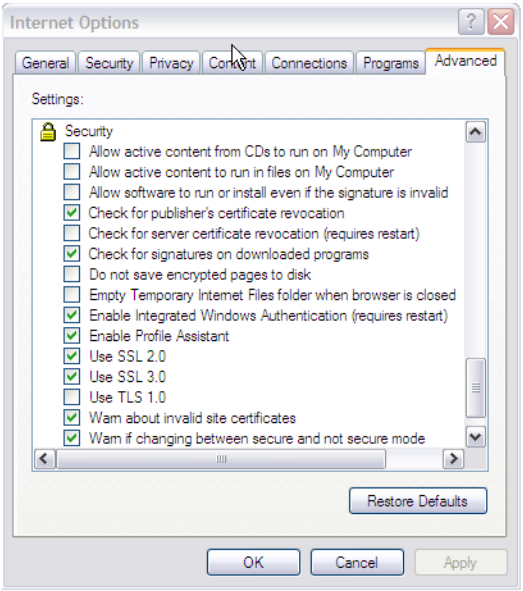

Figure 6: Internet Explorer 6 Internet Options Advanced Dialog

- Click on the **Advanced** tab of the Internet Options dialog.
- Click on the **Restore Defaults** button to assure the Security settings are appropriate for accessing the FSC BX600 Server Blade Chassis.
- Make sure the box labeled, *Do not save encrypted pages to disk* is **not** checked.
- Click **OK**.

2.3.5 MMB and DKVM certificate integration into the IE6 browser's store of trusted sites

The MMB embedded web server is an SSL enabled web server. When a web browser connects to an SSL enabled web server, the server sends the browser its SSL certificate. The web browser uses it to verify that the web server is actually the MMB server to whom the browser intended to communicate.

Each SSL certificate has paired with it a *private key*. That private key is kept secret by the legitimate web server, and it is never shared with anyone. No web server can use the SSL certificate to identify itself unless it is in possession of the corresponding private key.

For a web browser to believe the SSL certificate is legitimate, that certificate must be *signed* by a *trusted certificate authority* known in advance to the browser. Otherwise, you will see a "Security Alert" dialog box every time you access the MMB IP address or the MMB FQDN (Fully Qualified Domain Name).

To import MMB or DKVM certificates into IE6 browser store of trusted sites - simple way:

- Using the Window Explorer, find the file, *RemoteView CA Cert.der*.

- Double click on the **RemoteView CA Cert.der** certificate file.

The following dialog should be displayed

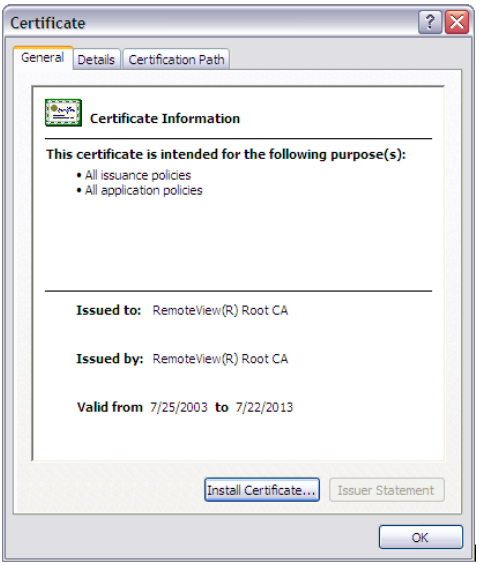

Figure 7: Certificate Information Dialog Box

- Click **Install Certificate** and follow the instructions of the Certificate Import Wizard.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

Figure 8: Internet Explorer 6 Certificate Import Wizard

- Click **Next**.

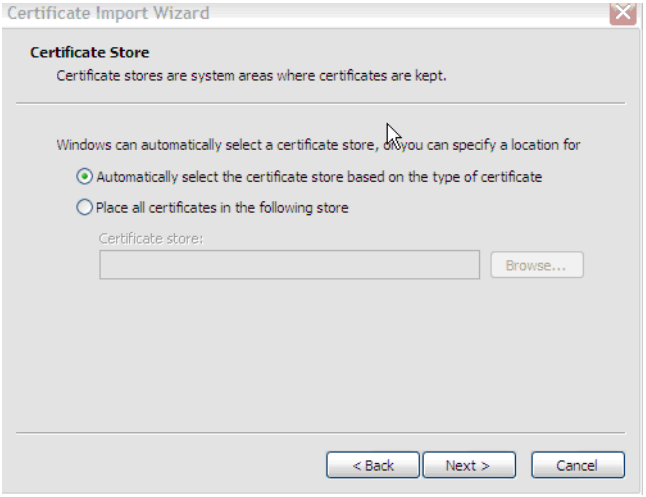
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

Figure 9: Internet Explorer 6 Certificate Import Wizard Store Dialog.

- Be sure to select the **Automatically select the certificate store based on the type of certificate** radio button.
- Click **Next**.

Figure 10: Internet Explorer 6 Completing the Certificate Import Wizard Dialog

- Click the **Finish** button to complete the importation of the trusted certificate. A warning similar to the following will appear:

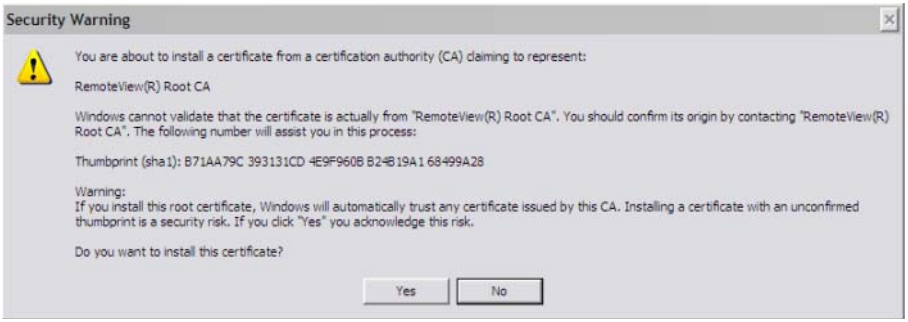
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
RemoteView(R) Root CA
Windows cannot validate that the certificate is actually from "RemoteView(R) Root CA". You should confirm its origin by contacting "RemoteView(R) Root CA". The following number will assist you in this process:
Thumbprint (sha1): B71AA79C 393131CD 4E9F960B B24B19A1 68499A28
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

Figure 11: Internet Explorer 6 Security Warning

- Click **Yes** to complete the installation of the certificate

To import MMB or DKVM certificates into IE6 browser store of trusted sites - alternate way:

The following method is for importing an MMB or dKVM certificate that has been signed by trusted certificate authority:

- Mouse click the **Tools** menu of the IE6 browser.
- Click on **Internet Options**.
- Click on the **Content** tab of the Internet Options dialog box.

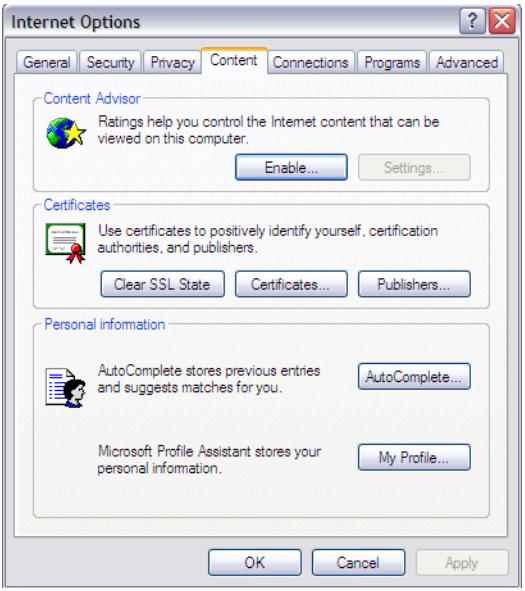

Figure 12: Internet Explorer 6 Internet Options Content Dialog

- Click the **Certificates** button. The Certificates Dialog appears.

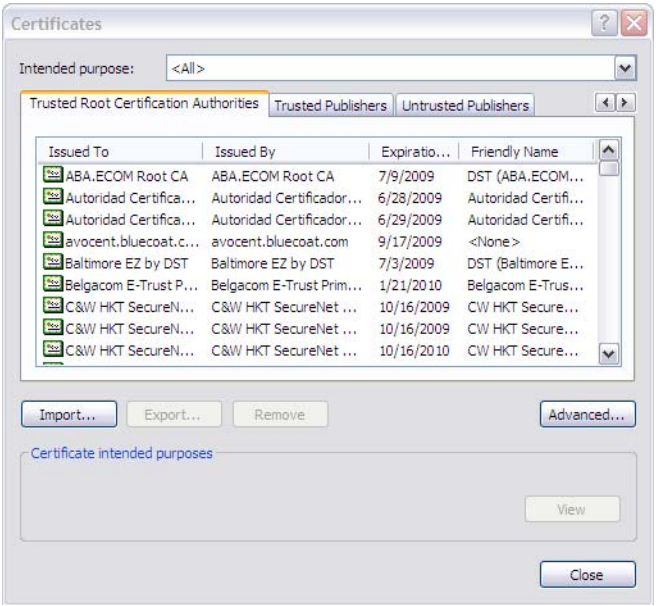

Figure 13: Internet Explorer 6 Certificates Dialog

- Click the **Import** button. The Certificate Import Wizard appears.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

Figure 14: Internet Explorer 6 Certificate Import Wizard

- Click **Next**.
- Browse to the location of the trusted certificate file and click on the name of the certificate or enter the fully specified path to the certificate filename in the *File name* field.

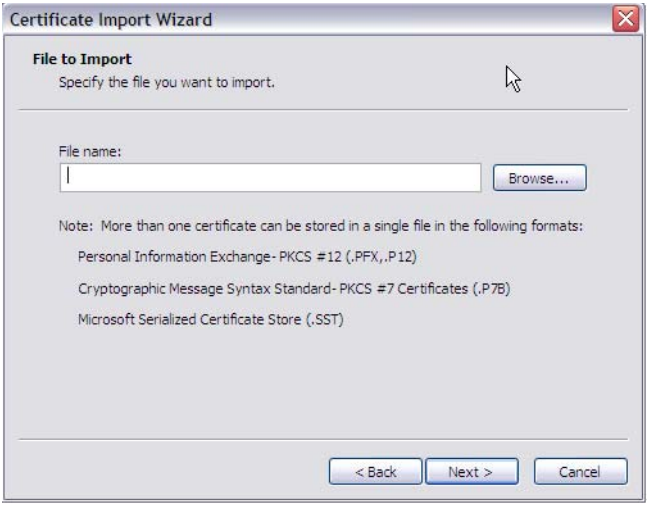
Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
< Back
Next >
Cancel

Figure 15: Internet Explorer 6 Certificate Import Wizard Browser

- Click **Next**.

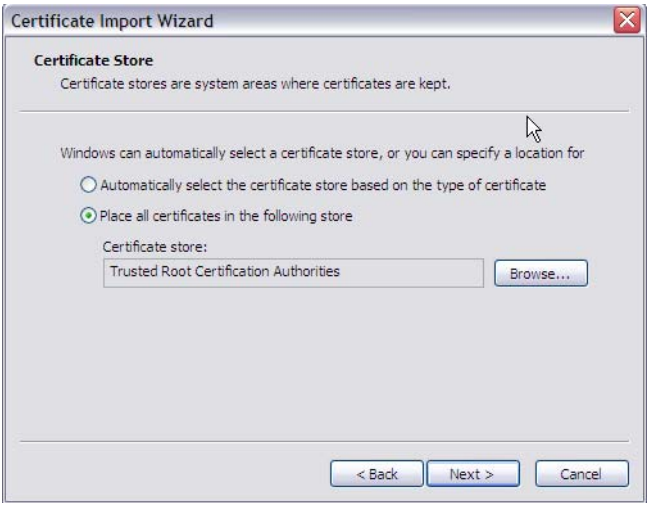
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
< Back
Next >
Cancel

Figure 16: Internet Explorer 6 Certificate Import Wizard Store Dialog.

- Click the **Place all certificates in the following store** radio button.
- Click the **Browse** button and select **Trusted Root Certification Authorities**
- Click the **Next** button to reveal the following dialog box.

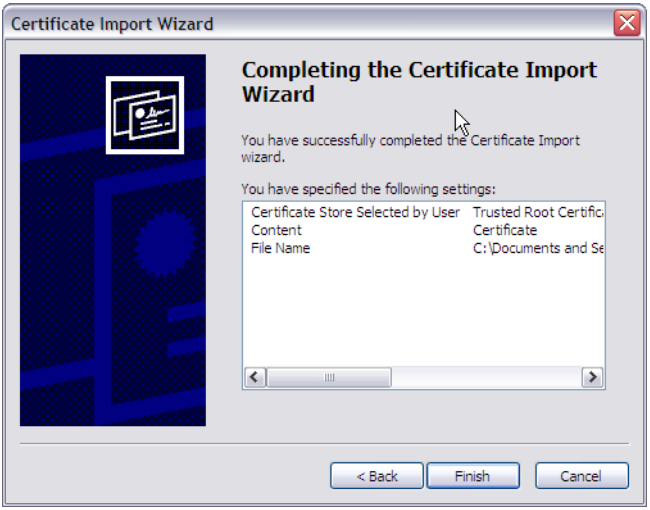

Figure 17: Internet Explorer 6 Certificate Import Wizard Complete

- Click **Finish**. A warning similar to the following will appear.

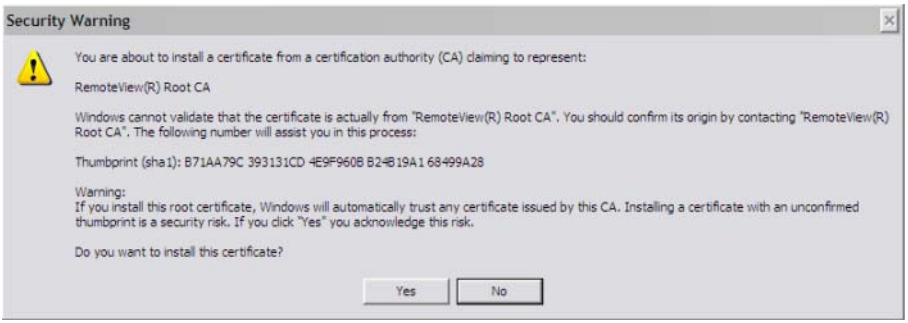
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
RemoteView(R) Root CA
Windows cannot validate that the certificate is actually from "RemoteView(R) Root CA". You should confirm its origin by contacting "RemoteView(R) Root CA". The following number will assist you in this process:
Thumbprint (sha1): B71AA79C 393131CD 4E9F960B B24B19A1 68499A28
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

Figure 18: Internet Explorer 6 Security Warning

- Click **Yes** to complete the installation of the certificate

2.4 Avoiding Security Alerts when Launching the Viewer

The dKVM embedded web server is also an SSL enabled web server. When the user launches the console viewer the MMB web server presents an SSL certificate to the dKVM. If the user sees a “Security Alert” dialog when launching the Console Viewer, the following steps for the appropriate browser can help eliminate the display of the “Security Alert” dialog box.

2.4.1 Internet Explorer 7 on Windows Vista Client

If any certificate error occurs when the browser tries to access the server, the browser will present the following dialog box.

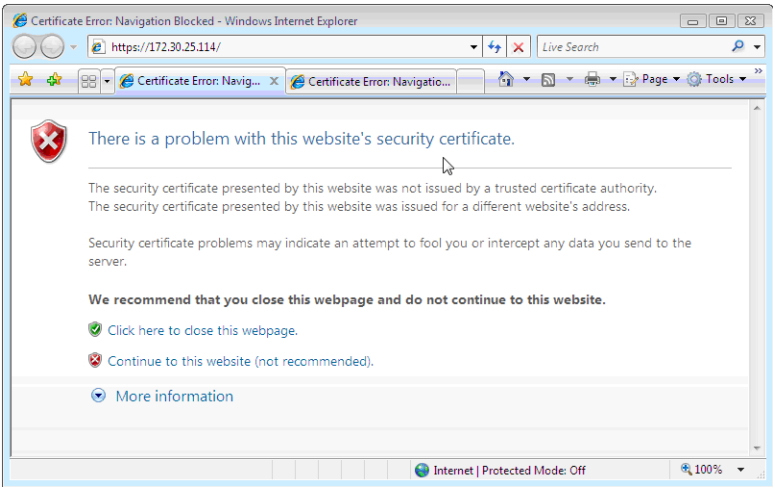
Certificate Error: Navigation Blocked - Windows Internet Explorer
https://172.30.25.114/
Live Search
Certificate Error: Navig...
Certificate Error: Navigatio...
Page
Tools
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information
Internet | Protected Mode: Off
100%

Figure 19: Internet Explorer 7 Certificate Error Dialog Box

This is the blocking page that will be displayed to warn of problems with a web server certificate.

To ignore the warning and continue:

If you choose to ignore this warning and continue, the Address bar will turn red with the message, “Certificate Error” at the right.

Click **Continue to this website (not recommended)** on the certificate error blocking page to ignore the warning and go the website.

Internet Explorer 7 will go to the requested web page and remember the certificate while you have your browser open. You can return to the site and will not receive another warning for that certificate until Internet Explorer 7 is restarted. However, you will still see the red address bar with the “Certificate Error” message to the right as shown in the figure below.

NOTE: You cannot turn off the Security Alerts in Internet Explorer 7.

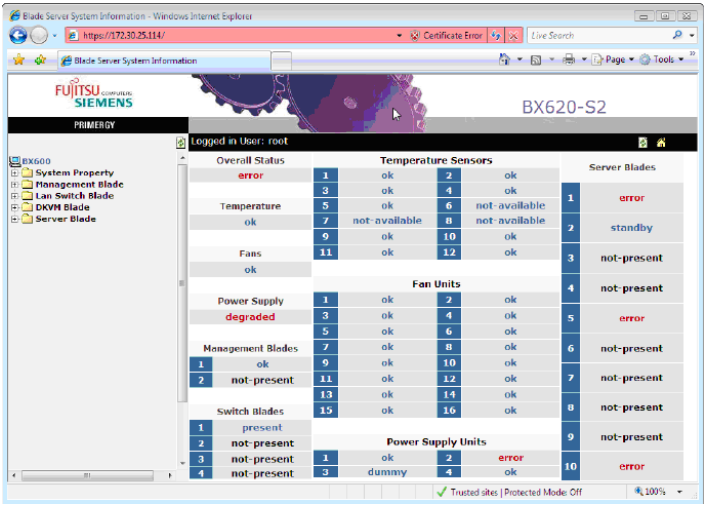

Figure 20: Blade Server System Information Screen with IE 7 Certificate Error

2.4.2 Internet Explorer 6 on Windows Client

If the certificate is not signed by a trusted certificate authority that the browser recognizes, then the browser may present the following Security Alert dialog box.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 21: Internet Explorer 6 First Security Alert Dialog

The first warning on the Security Alert dialog is:

> The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The occurrence of this first warning can be eliminated by viewing the certificate, importing the certificate and then placing it in the Trusted Root Certification Authorities certificate store of the IE 6 browser.

- Click the *View Certificate* button. You will see the following:

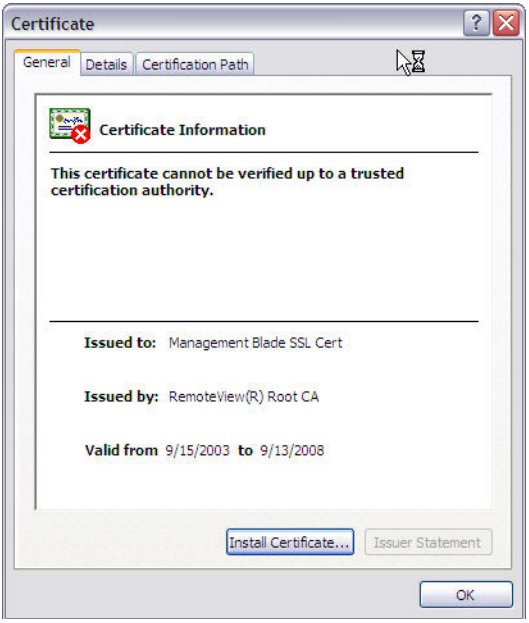

Figure 22: Certificate Information Dialog

- Click **Install Certificate** and follow the instructions of the Certificate Import Wizard.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

Figure 23: Certificate Import Wizard

- Click the **Next** button.

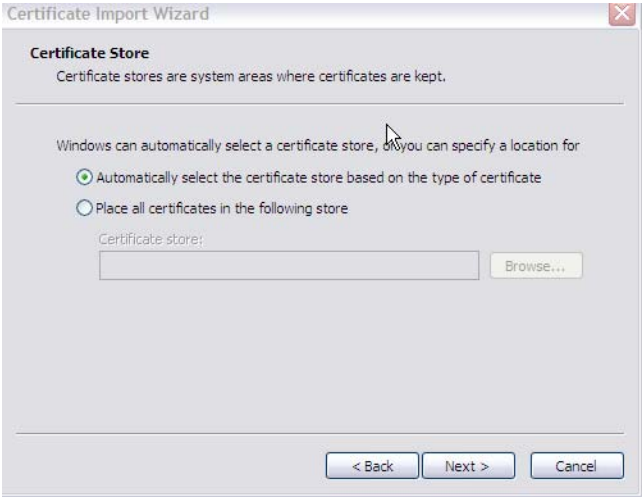
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

Figure 24: Certificate Store Page of Certificate Wizard

- Click the **Next** button.

Figure 25: Completing the Certificate Import Wizard

- Click **Finish**. You should see a warning similar to the following:

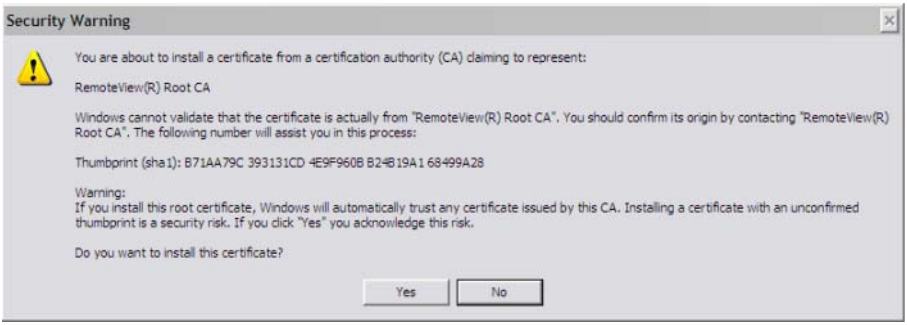
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
RemoteView(R) Root CA
Windows cannot validate that the certificate is actually from "RemoteView(R) Root CA". You should confirm its origin by contacting "RemoteView(R) Root CA". The following number will assist you in this process:
Thumbprint (sha1): B71AA79C 393131CD 4E9F960B B24B19A1 68499A28
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

Figure 26: Security Warning Dialog

- Click **Yes** to complete the installation of the certificate.

If the last warning on the Security Alert dialog box is:

> The name on the security certificate is invalid or does not match the name of the site.

It can only be removed by using a signed SSL Certificate whose name matches the URL name assigned to the MMB web server.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 27: Security Alert with Name not Matching Site

- This can be done by:
  - Adding an entry to your Domain Name Server (DNS) for the MMB that maps its Fully Qualified Domain Name (FQDN) to its IP address. (e.g., https://fsc-management-blade resolves to 192.168.0.12)
  - generating a Certificate whose Common Name (CN) matches the Fully Qualified Domain Name (FQDN) assigned to the MMB web server,
  - submitting a “Certificate Signing Request” to a Trusted Third Party Certificate Authority and
  - uploading the requested signed certificate from the Trusted Third Party Certificate Authority to the MMB web server.

Now if you specify the MMB FQDN[1] when accessing the MMB via the Internet Explorer browser, there should not be a Security Alerts dialog box displayed.

If you don't have a third party certificate, simply confirm the alert by clicking the Yes button and the Security Alert dialog will not appear upon subsequent openings of the remote console session after the initial remote console session.

The very first time you try to launch the console viewer you will see the Java Web Start dialog box appear

The Java Web Start applet will begin its one-time initial download of the viewer application.

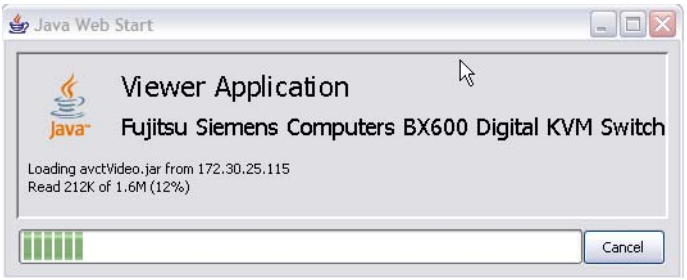

Figure 28: Java Web Start Dialog Box

Finally the viewer application presents its signed certification for verification and asks the user for permission to run the application.

- Click the **Always trust content from this publisher** checkbox to avoid the display of the Warning - Security dialog box upon subsequent launches of the console viewer application.

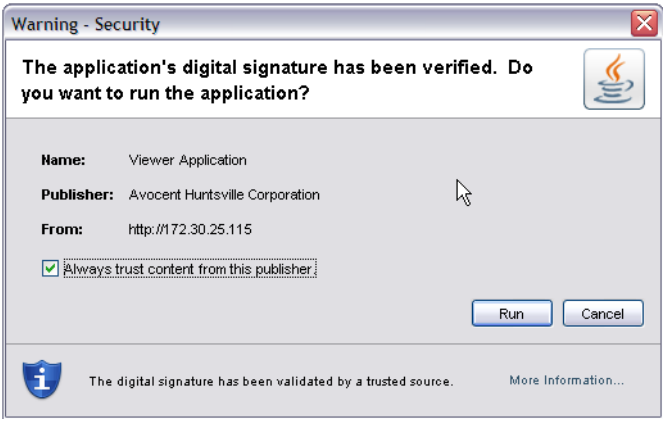
Warning - Security
The application's digital signature has been verified. Do you want to run the application?
Name: Viewer Application
Publisher: Avocent Huntsville Corporation
From: http://172.30.25.115
Always trust content from this publisher
Run
Cancel
The digital signature has been validated by a trusted source.
More Information...

Figure 29: Java Warning - Security Dialog Box

1. As an example, https://fsc-management-blade could be an FQDN.

- Click the **Run** button to launch the Viewer Console Application.

  The next window displayed should be a Remote Viewer Console Application similar to the one shown below.

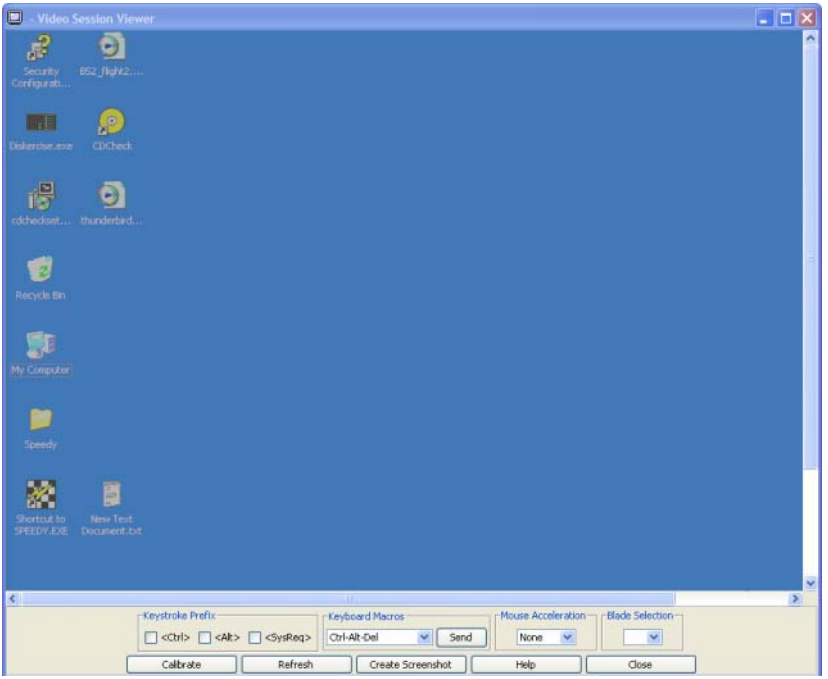

Figure 30: Digital KVM Viewer Application Window

2.4.3 Mozilla Firefox 1.5 on Red Hat 4

Before getting started make sure the Firefox browser is configured to interface with SSL and is configured to automatically select the security certificate to be presented to a requesting web site.

- Click in succession on the Firefox browser pull-down menu: **Edit** - **Preferences**. This will bring up the Firefox Preferences dialog box.
- Click the **Advanced** icon.

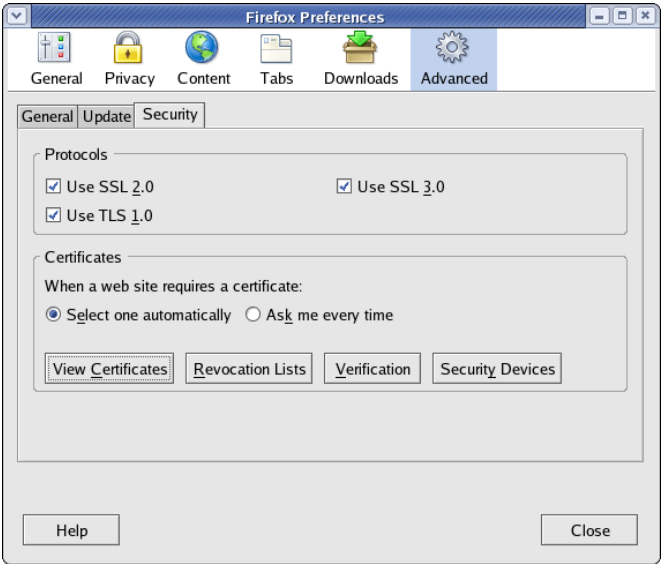

Figure 31: Firefox Preferences Dialog Box

- Click the **View Certificates** button. The Certificate Manager will appear as shown below.

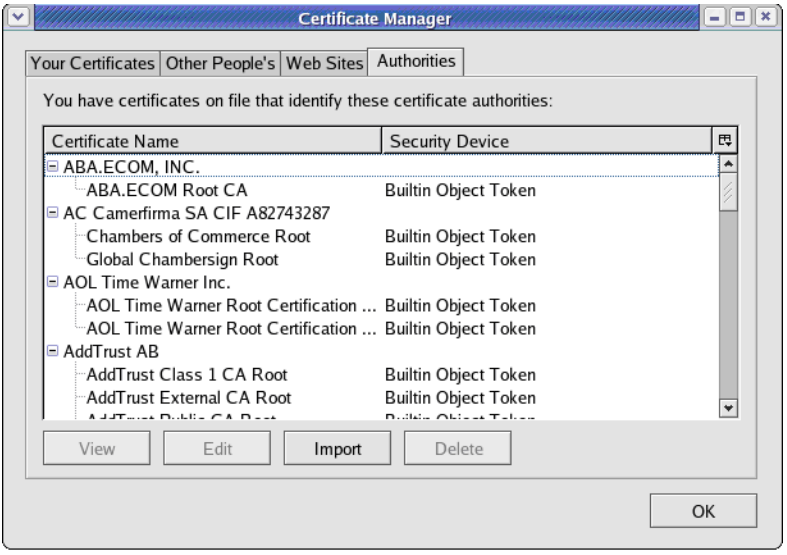

Figure 32: Firefox Certificate Manager Dialog Box

- Click the **Import** button to import the RemoteView CA Cert certificate. A Select File dialog box with a CA certificate selection will appear.

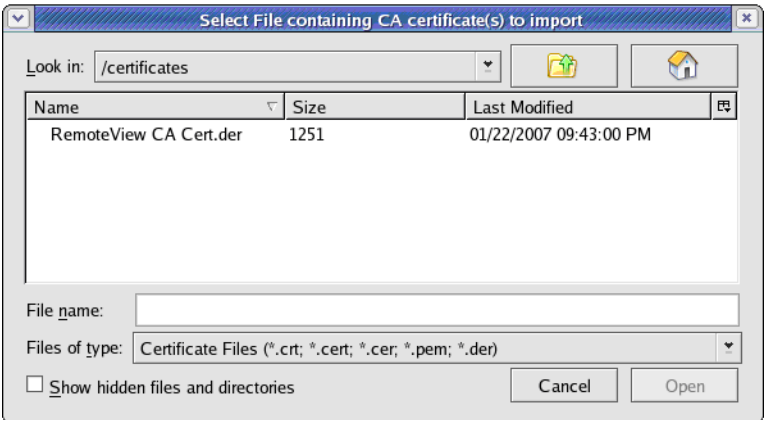

Figure 33: Firefox Certificate Import Selection Dialog Box

- Use the folder icon to locate the directory containing the RemoteView CA Cert.der file.

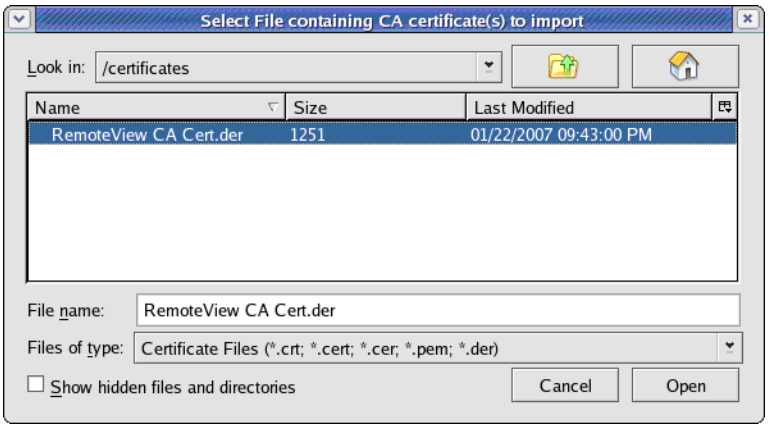

Figure 34: Highlighting the Certificate to be Imported

- Highlight the name of the file (RemoteView CA Cert.der).

  -or-

  Enter the file name into the File name field in the import selection dialog box.
- Click **Open**. A Downloading Certificate dialog box will appear.

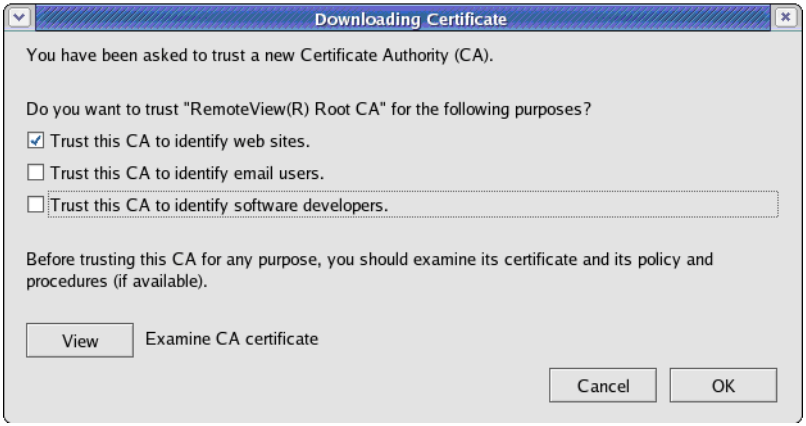
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "RemoteView(R) Root CA" for the following purposes?
Trust this CA to identify web sites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
Cancel
OK

Figure 35: Downloading Certificate Dialog Box

- Click the **Trust this CA to identify web sites** checkbox.
- Click the **OK** button. The Ceftificate Manager dialog box will reappear.

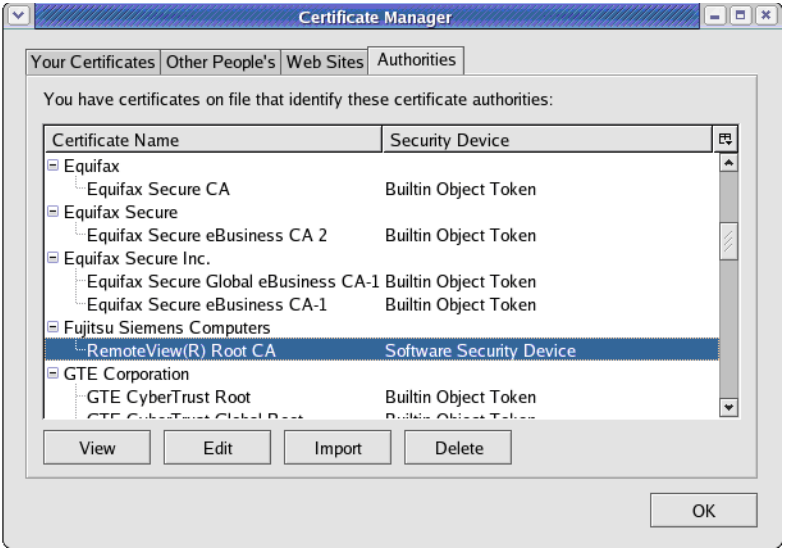

Figure 36: Certificate Confirmation

- Use the scrollbar to find and confirm the correct certificate has been imported to the Firefox browser.

To manage past certificates from websites that have been accepted by the browser:

- Clicking the **View** button of the browser's Certificate Manager. The resultant dialog is shown below.

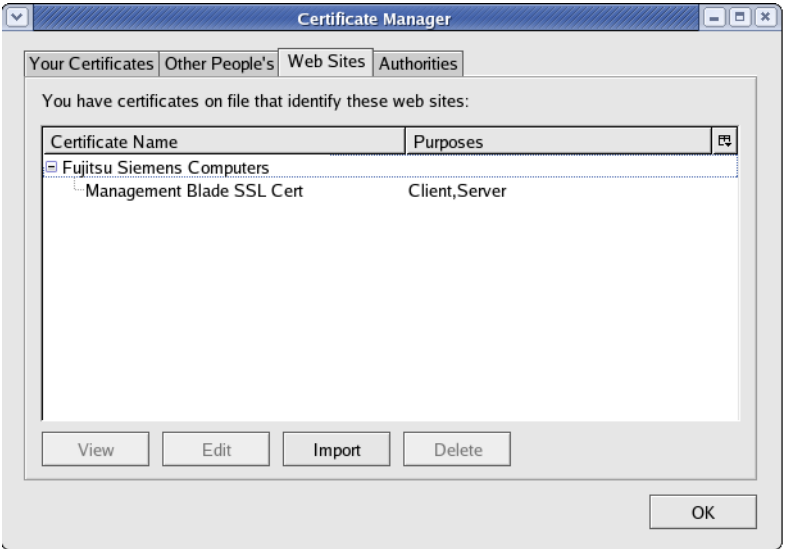

Figure 37: Viewing Certificates and their Associated Web Sites

- Click the **Web Sites** tab to view a list of certificates and their associated web sites.

  If the certificate is not signed by a trusted certificate authority that the browser recognizes, then the browser may present the following Web site Certified by an Unknown Authority dialog box.

Website Certified by an Unknown Authority
Unable to verify the identity of Management Blade SSL Cert as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Management Blade SSL Cert, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site Management Blade SSL Cert?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
Cancel
OK

Figure 38: Firefox Certified by Unknown Authority Dialog Box

- Click the **Examine Certificate** button to find out why the certificate is not recognized.

Security Error: Domain Name Mismatch
You have attempted to establish a connection with "172.30.25.115". However, the security certificate presented belongs to "Management Blade SSL Cert". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "172.30.25.115", please cancel the connection and notify the site administrator.
View Certificate
Cancel
OK

Figure 39: Firefox Domain Name Mismatch Dialog

- Click the **View Certificate** button to find all of the certificates involved in the SSL handshake.
- Click **OK** after you are satisfied that the security certificate belongs to the web server you are trying to access.

  The next time you get the “Website Certified by an Unknown Authority” dialog, click the option **Accept this certificate permanently**.[1]

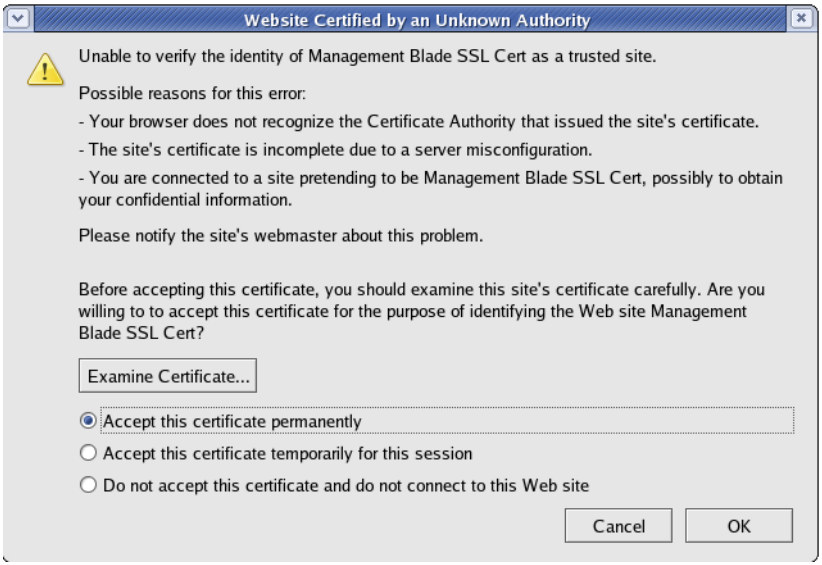
Website Certified by an Unknown Authority
Unable to verify the identity of Management Blade SSL Cert as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Management Blade SSL Cert, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site Management Blade SSL Cert?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
Cancel
OK

Figure 40: Accepting Firefox Website Certificate

Thereafter there should be no Security Alert dialogs displayed when the browser connects to the MMB web server.

1. Make sure you specify a FQDN for the MMB (e.g., https://fsc-management-blade).

The first time the user tries to launch the console viewer the user will be prompted by the following dialog box.

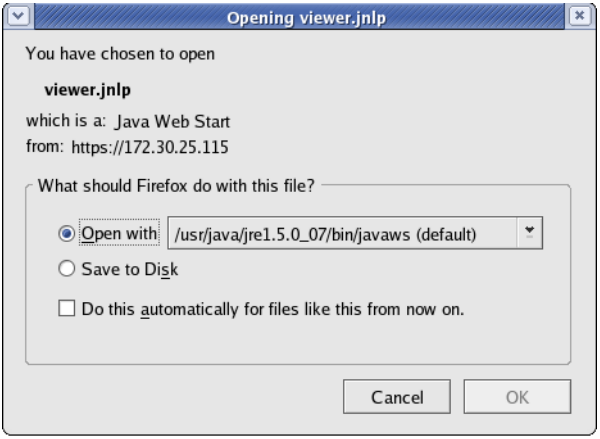

Figure 41: Firefox Opening Viewer.jnlp Dialog Box

- Click the **Do this automatically for files like this from now on** checkbox.
- Click **OK** to load the *viewer.jnlp* binary. After the.jnlp file is loaded, you should not be prompted by this dialog again.

  The next window displayed should be a Remote Viewer Console Application similar to the one shown below.

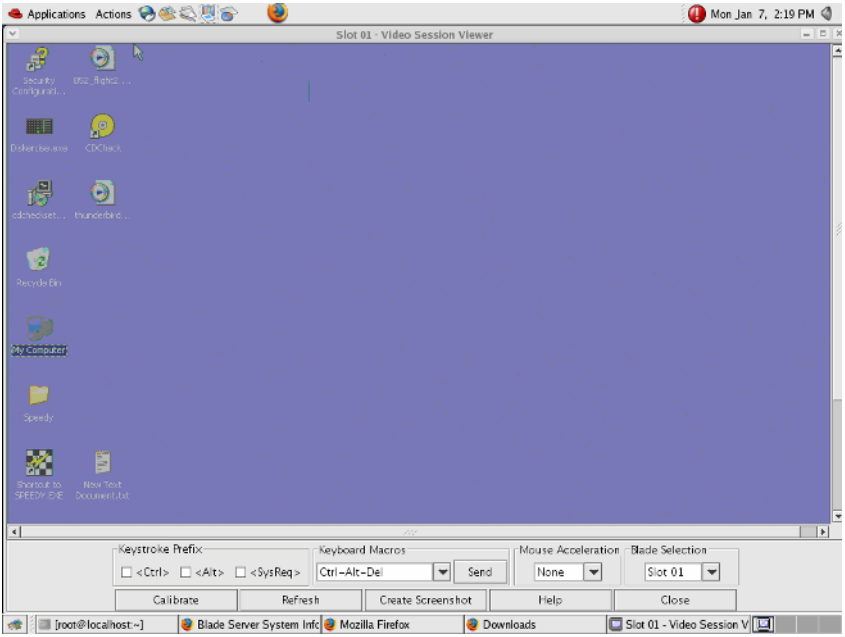

Figure 42: Firefox dKVM Viewer Window

2.4.4 Mozilla 1.7.12 on Red Hat 4

Before getting started make sure the Mozilla browser is configured to interface with SSL and is configured to automatically select the security certificate to be presented to a requesting web site.

- Click in succession on the Mozilla browser pulldown menu: **Edit - Preferences**. This will bring up the Mozilla Preferences dialog box.
- Click the **Privacy & Security** plus sign in the left column to expand the category.
- Click the **Certificates** subcategory.

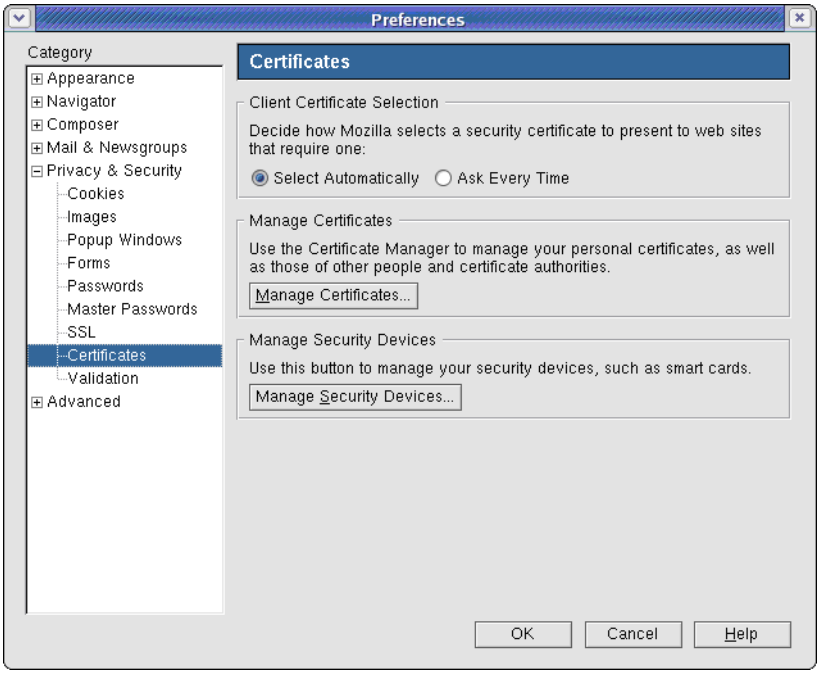

Figure 43: Selecting Certificates in Mozilla Preferences

- Click the **Manage Certificates** button to launch the Certificate Manager.

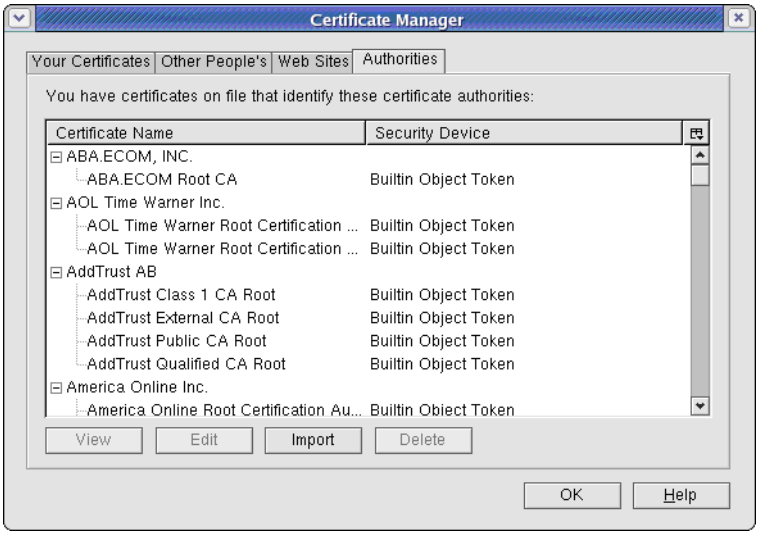

Figure 44: Mozilla Certificate Manager Authorities List

- Click the **Import** button to select the *RemoteView CA Cert.der* certificate.

The Mozilla Certificate Import Selection Dialog Box will appear.

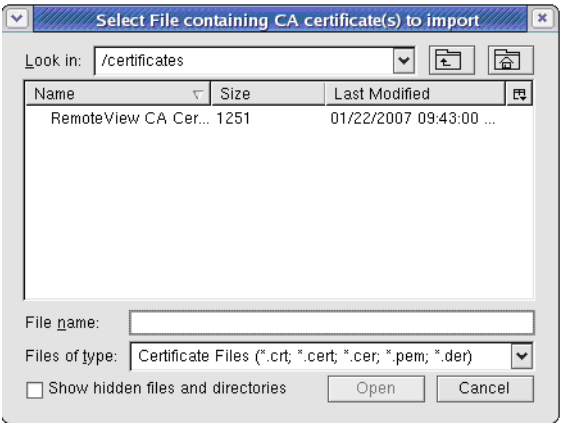

Figure 45: Mozilla Certificate Import Selection Dialog Box

- Use the folder icon to locate the directory containing the *RemoteView CA Cert.der* file.

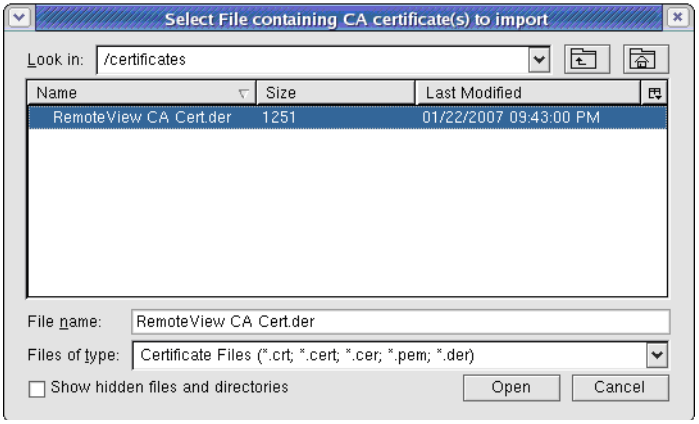

Figure 46: Entering the Certificate File Name

- Enter the file name of the certificate (RemoteView CA Cert.der) in the **File name** field.
- Click **Open**. A Downloading Certificate dialog box will appear.

Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "RemoteView(R) Root CA" for the following purposes?
Trust this CA to identify web sites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
OK
Cancel
Help

Figure 47: Downloading Certificate Dialog Box

- Click the **Trust this CA to identify web site** checkbox.
- Click the **OK** button. The Certificate Manager dialog box will reappear.

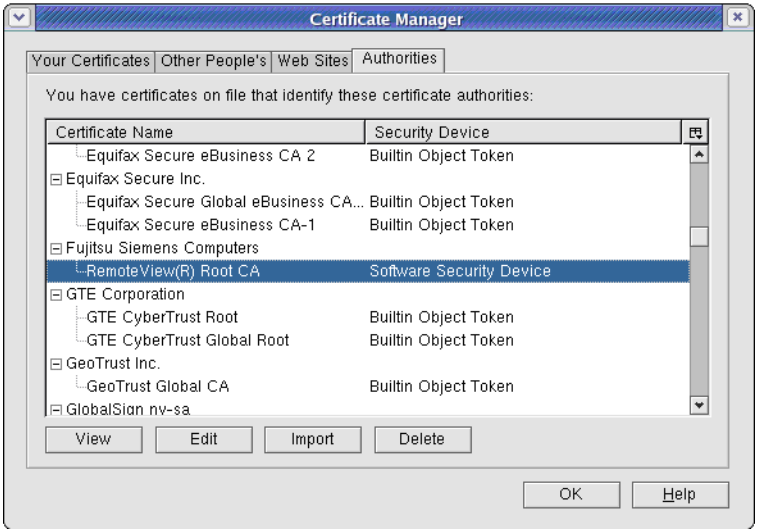

Figure 48: Confirming the Certificate

- Use the scrollbar to find and confirm that the correct certificate has been imported to the Mozilla browser.

  If the certificate is not signed by a trusted certificate authority that the browser recognizes, then the browser may present the following Website Certified by an Unknown Authority dialog box.

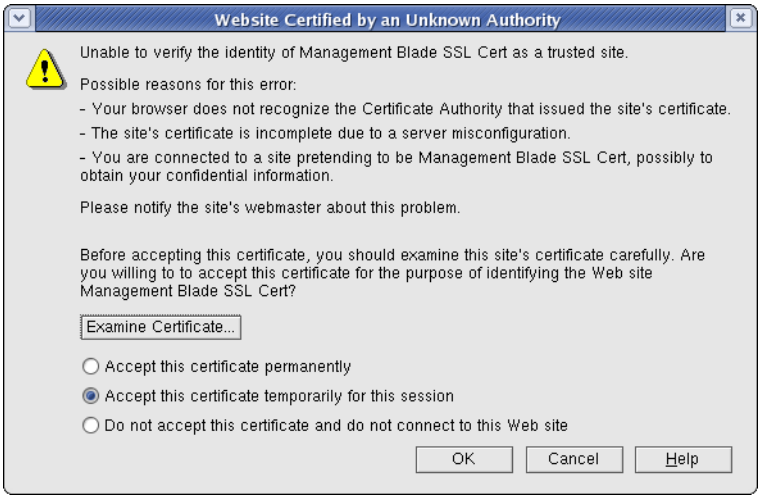
Website Certified by an Unknown Authority
Unable to verify the identity of Management Blade SSL Cert as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Management Blade SSL Cert, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site Management Blade SSL Cert?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

Figure 49: Red Hat Mozilla Certified by Unknown Authority Dialog Box

- Click the **Examine Certificate** button to find out why the certificate is not recognized. A Security Error Domain Name Mismatch dialog box will appear.

Security Error: Domain Name Mismatch
You have attempted to establish a connection with "172.30.25.115". However, the security certificate presented belongs to "Management Blade SSL Cert". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "172.30.25.115", please cancel the connection and notify the site administrator.
View Certificate
OK
Cancel
Help

Figure 50: Red Hat Mozilla Domain Name Mismatch Dialog

- Click the **View Certificate** button to find all of the certificates involved in the SSL handshake.
- Click **OK** after you are satisfied that the security certificate belongs to the web server you are trying to access.

  The next time you get the Website Certified by an Unknown Authority dialog, click the option to **Accept this certificate permanently**.[1]

1. Make sure you specify a FQDN for the MMB (e.g., https://fsc-management-blade).

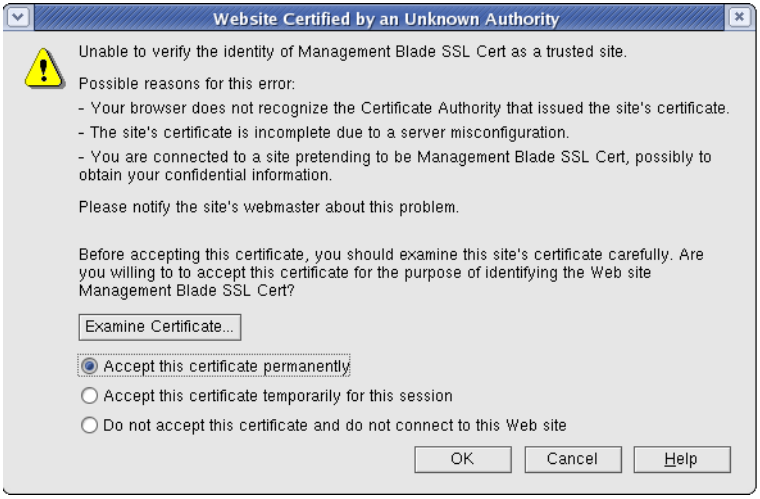
Website Certified by an Unknown Authority
Unable to verify the identity of Management Blade SSL Cert as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Management Blade SSL Cert, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site Management Blade SSL Cert?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

Figure 51: Accepting Red Hat Mozilla Web site Certificate

Thereafter there should be no Security Alert dialogs displayed when the browser connects to the MMB web server.

The first time the user tries to launch the console viewer the user will be prompted by the following dialog.

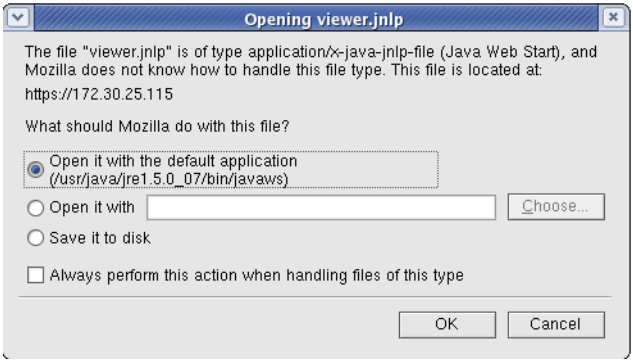
Opening viewer.jnlp
The file "viewer.jnlp" is of type application/x-java-jnlp-file (Java Web Start), and Mozilla does not know how to handle this file type. This file is located at:
https://172.30.25.115
What should Mozilla do with this file?
Open it with the default application (/usr/java/jre1.5.0_07/bin/javaws)
Open it with
Choose...
Save it to disk
Always perform this action when handling files of this type
OK
Cancel

Figure 52: Red Hat Mozilla Opening Viewer.jnlp Dialog

- Click on the **Always perform this action when handling files of this type** checkbox.
- Click **OK** to load the *viewer.jnlp* binary. After the .jnlp file is loaded, you should not be prompted by this dialog again.

  The next window displayed should be a Remote Viewer Console Application similar to the one shown below.

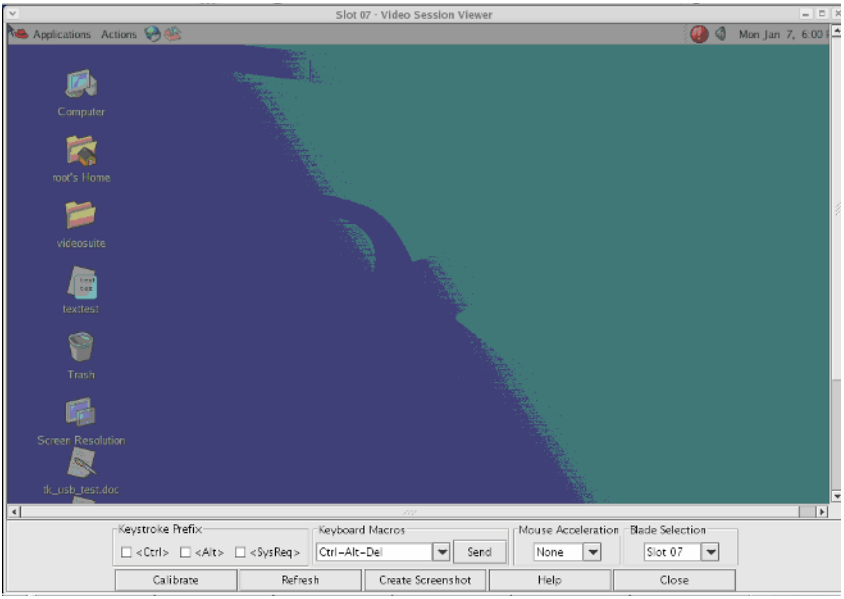

Figure 53: Red Hat Mozilla dKVM Viewer Window

2.4.5 Mozilla 1.7.5 on SUSE9

Before getting started make sure the Mozilla browser is configured to interface with SSL and is configured to automatically select the security certificate to be presented to a requesting web site.

- Click in succession on the Mozilla browser pulldown menu: **Edit - Preferences**. This will bring up the Mozilla Preferences dialog box.
- Click the **Privacy & Security** plus sign in the left column to expand the category.
- Click the **Certificates** subcategory.

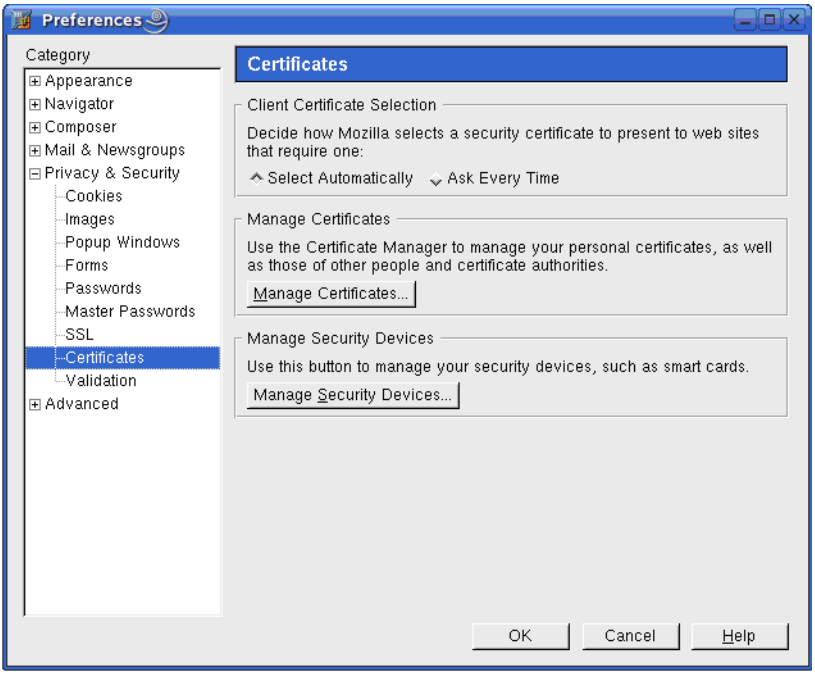

Figure 54: Selecting Certificates in Mozilla Preferences

- Click the **Manage Certificates** button to launch the Certificate Manager.

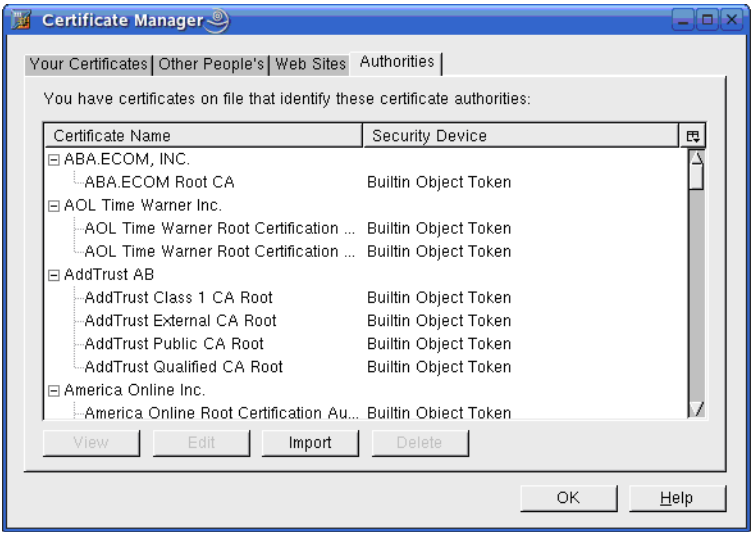

Figure 55: Mozilla Certificate Manager Authorities List

- Click the **Import** button to select the *RemoteView CA Cert.der* certificate.

The Mozilla Certificate Import Selection Dialog Box will appear.

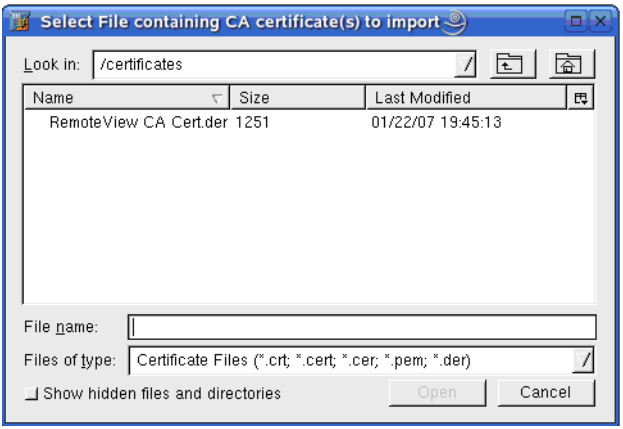

Figure 56: Mozilla Certificate Import Selection Dialog Box

- Use the folder icon to locate the directory containing the *RemoteView CA Cert.der* file.

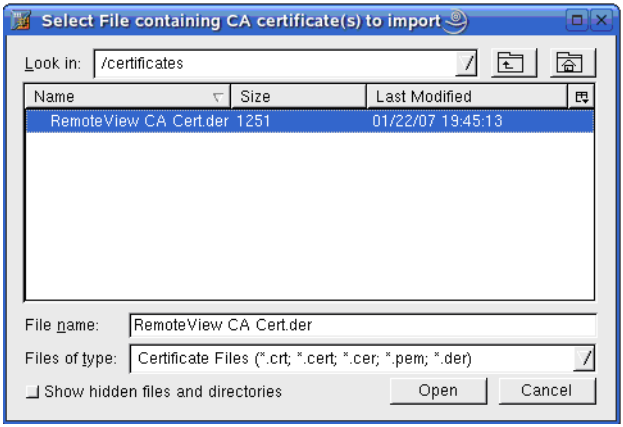

Figure 57: Entering the Certificate File Name

- Enter the file name of the certificate (RemoteView CA Cert.der) in the **File name** field.
- Click **Open**. A Downloading Certificate dialog box will appear.

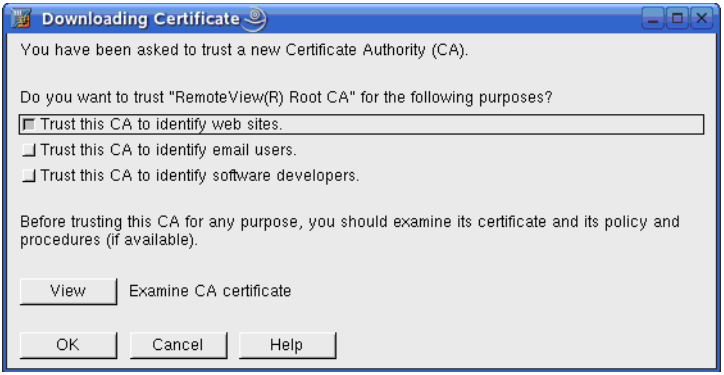
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "RemoteView(R) Root CA" for the following purposes?
Trust this CA to identify web sites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
OK
Cancel
Help

Figure 58: Downloading Certificate Dialog Box

- Click the **Trust this CA to identify web site** checkbox.
- Click the **OK** button. The Certificate Manager dialog box will reappear.

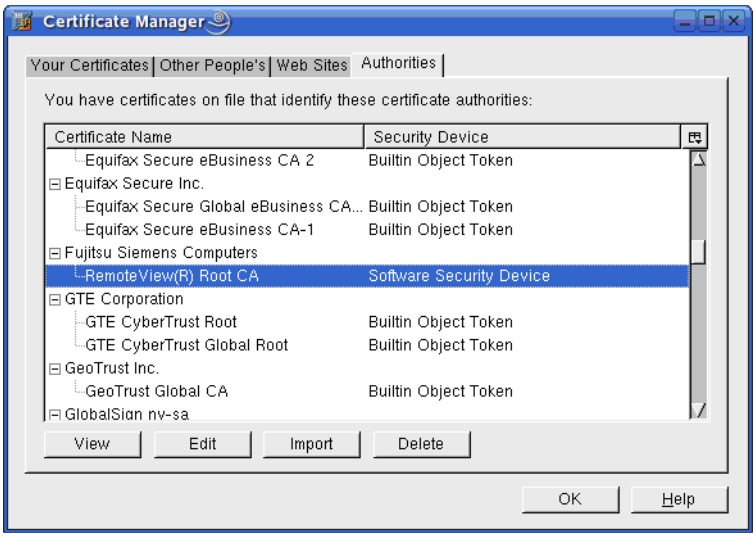

Figure 59: Confirming the Certificate

- Use the scrollbar to find and confirm that the correct certificate has been imported to the Mozilla browser.

  If the certificate is not signed by a trusted certificate authority that the browser recognizes, then the browser may present the following Website Certified by an Unknown Authority dialog box.

Website Certified by an Unknown Authority
Unable to verify the identity of Management Blade SSL Cert as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Management Blade SSL Cert, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site Management Blade SSL Cert?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

Figure 60: SUSE Mozilla Certified by Unknown Authority Dialog

Click the **Examine Certificate** button to find out why the certificate is not recognized. A Security Error Domain Name Mismatch dialog box will appear.

Security Error: Domain Name Mismatch
You have attempted to establish a connection with "172.30.25.115". However, the security certificate presented belongs to "Management Blade SSL Cert". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "172.30.25.115", please cancel the connection and notify the site administrator.
View Certificate
OK
Cancel
Help

Figure 61: SUSE Mozilla Domain Name Mismatch Dialog

- Click the **View Certificate** button to find all of the certificates involved in the SSL handshake.
- Click **OK** after you are satisfied that the security certificate belongs to the web server you are trying to access.

  The next time you get the Website Certified by an Unknown Authority dialog, click the option **Accept this certificate permanently**.[1]

1. Make sure you specify a FQDN for the MMB (e.g., https://fsc-management-blade).

Website Certified by an Unknown Authority
Unable to verify the identity of Management Blade SSL Cert as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Management Blade SSL Cert, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site Management Blade SSL Cert?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

Figure 62: Accepting SUSE Mozilla Web site Certificate

Thereafter there should be no Security Alert dialogs displayed when the browser connects to the MMB web server.

The first time the user tries to launch the console viewer the user will be prompted by the following dialog.

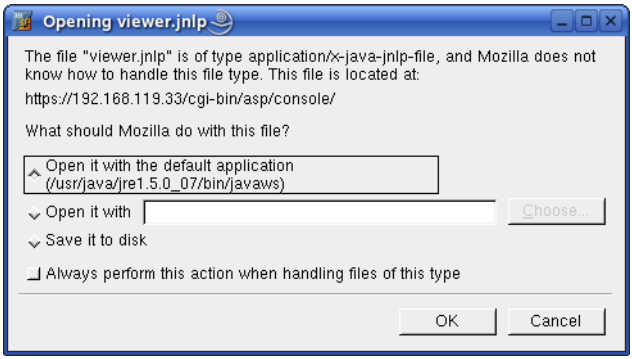
Opening viewer.jnlp
The file "viewer.jnlp" is of type application/x-java-jnlp-file, and Mozilla does not know how to handle this file type. This file is located at:
https://192.168.119.33/cgi-bin/asp/console/
What should Mozilla do with this file?
Open it with the default application (/usr/java/jre1.5.0_07/bin/javaws)
Open it with
Choose...
Save it to disk
Always perform this action when handling files of this type
OK
Cancel

Figure 63: SUSE Mozilla Opening Viewer.jnlp Dialog

- Click the square box labeled, **Always perform this action when handling files of this type**.
- Click **OK** to load the *viewer.jnlp* binary. After the .jnlp file is loaded, you should not be prompted by this dialog again.

  You will see the Download Manager dialog display after the jnlp binary is successfully downloaded.

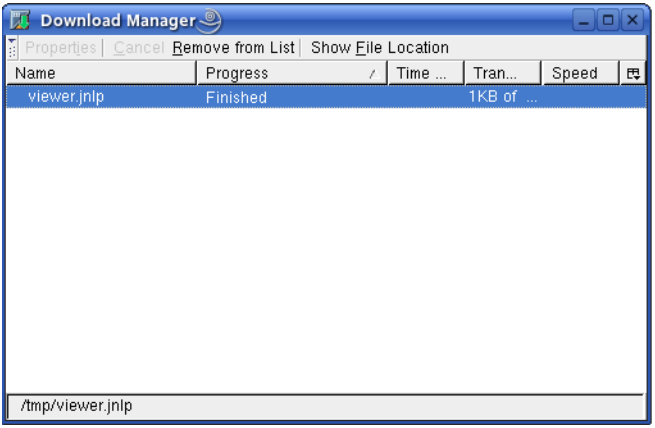

Figure 64: SUSE Mozilla Download Manager

The Java viewer .jar file will begin its one-time initial download.

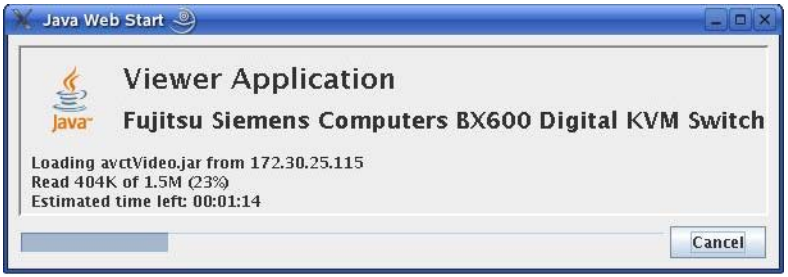

Figure 65: SUSE Mozilla Java Web Start Indicator

Finally, the viewer application presents its signed certificate for verification and asks the user for permission to run the application.

Warning - Security
The application's digital signature has been verified. Do you want to run the application?
Java
Name: Viewer Application
Publisher: Avocent Huntsville Corporation
From: http://172.30.25.115
Always trust content from this publisher.
Run
Cancel
The digital signature has been validated by a trusted source.
More Information...

Figure 66: SUSE Mozilla Java Security Dialog

- Click the **Always trust content from this publisher** checkbox to avoid seeing the Warning - Security dialog after this instance.
- Click the **Run** button to launch a Viewer Console Session similar to the display below.

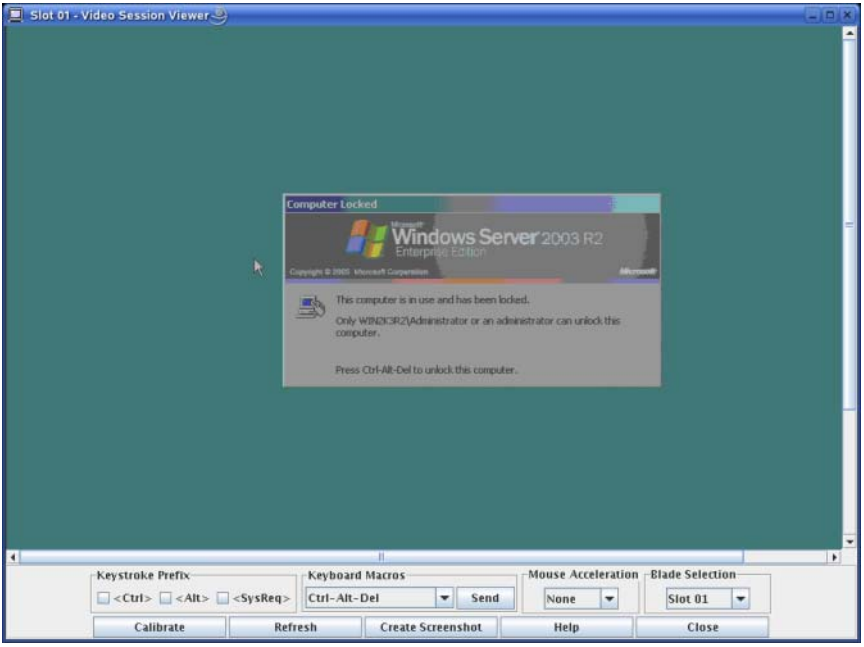

Figure 67: SUSE Mozilla dKVM Viewer Window

2.5 Finding the dKVM IP-address when using DHCP

The dKVM IP address is displayed on the KVM Configuration web page. To get there, do the following:

- Point your browser to the MMB IP Address to get the primary Blade Server System Information web page shown below.

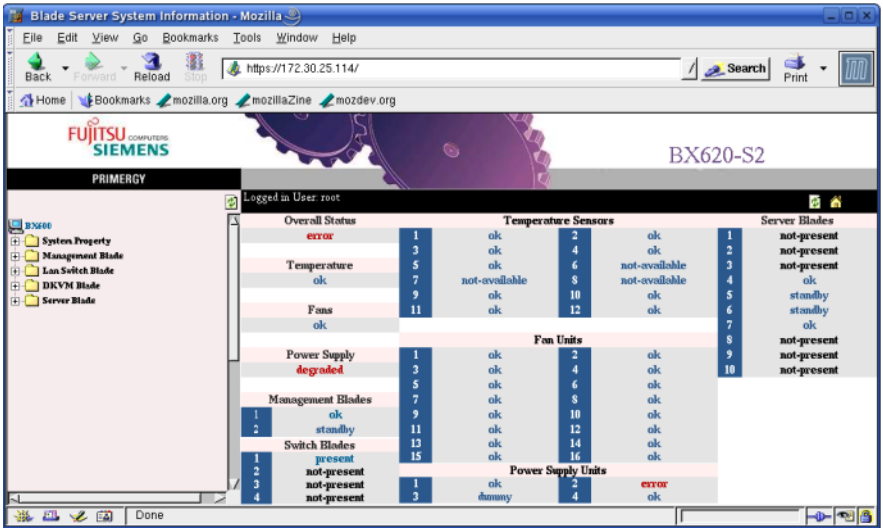

Figure 68: Primary Blade Server System Information Web Page

- Use your mouse to click on the **plus sign** next to the *DKVM Blade* folder on the left side of the web page.
- Click the **Network Configuration** file icon to display the KVM Configuration web page shown below.

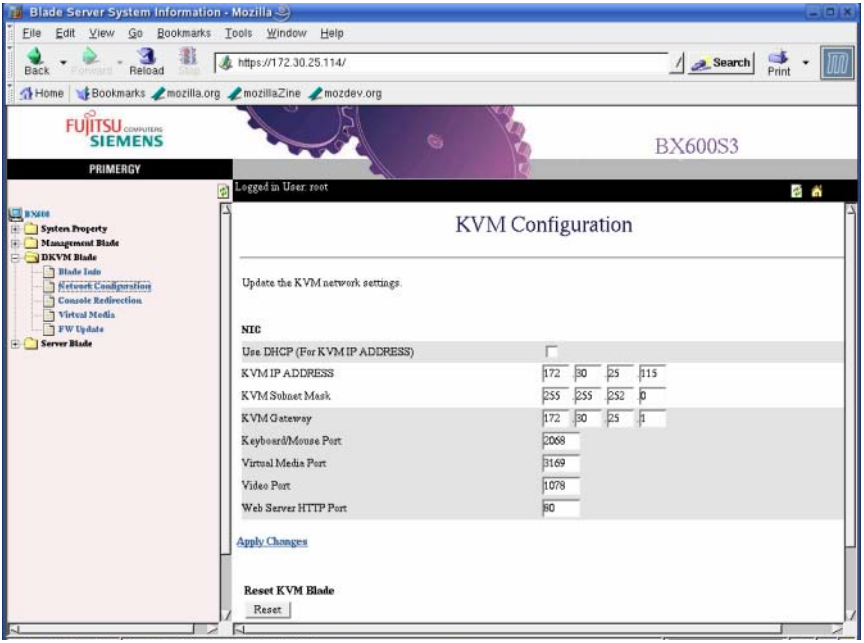

Figure 69: KVM Configuration Web Page

You should see the assigned KVM IP Address displayed on this page.

2.5.1 Integrating the DKVM IP address with https setting

There is no need to integrate the DKVM IP address with the https setting. Once the 'HTTP SSL' is enabled on the LAN Interface web page, the DKVM IP address does not have to be integrated with the https setting.

2.5.2 Resolutions supported by the DKVM Console Viewer

Analog video detected and provided to the remote console viewer will be in the range of 640 x 480 to 1024 x 768. The video resolutions supported will be as follows:

Resolution	Refresh Rate	Horizontal Freq
640X480	60Hz	31.5KHz
	72Hz	37.9KHz
	75Hz	37.5KHz
	85Hz	43.3KHz
800X600	60Hz	37.9KHz
	72Hz	48.1KHz
	75Hz	46.9KHz
	85Hz	53.7KHz
1024X768	60Hz	48.4KHz
	72Hz	56.5KHz
	75Hz	60.0KHz
	85Hz	68.7KHz
1280X1024	60Hz	64.0KHz

3 Installation

You can deploy the BX600 Digital KVM Switch Module into most existing KVM infrastructures. In addition, you can set up the BX600 Digital KVM Switch in tiers from Fujitsu Siemens branded KVM appliances such as the Fujitsu Siemens s3-1621 Console Switch and analog s2-0801 and s2-1602 switches. It can also be tiered from other industry products that support the OSCAR interface.

3.1 Configuring the BX600 Digital KVM Switch

Before using the BX600 Digital KVM Switch or configuring it into tiers, you must first set it up for basic use. Figure 70 displays a basic configuration for the BX600 Digital KVM Switch.

To connect the BX600 Digital KVM Switch:

- Connect the local KVM cable to the appropriate port on the BX600 Digital KVM Switch.
- Connect the keyboard, monitor, and mouse to the local KVM cable.

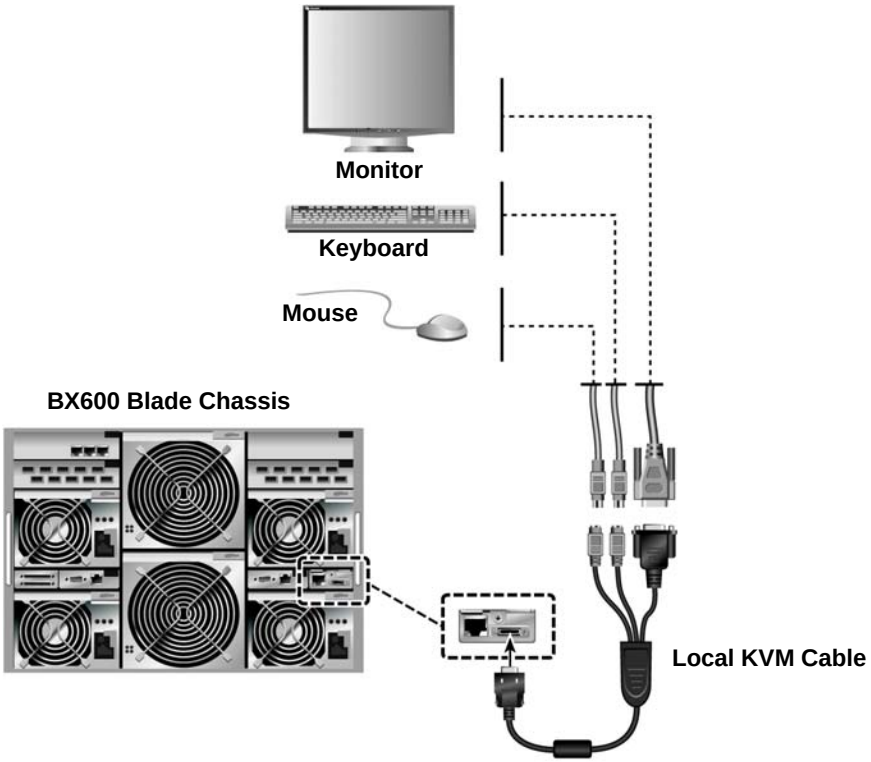

Figure 70: BX600 Digital KVM Switch Basic Configuration

To display the BX600 Digital KVM Switch Main dialog box by slot order:

- Press Print Screen to launch the OSCAR interface.
- Click **Setup** and then click **Menu**. The Menu dialog box appears.

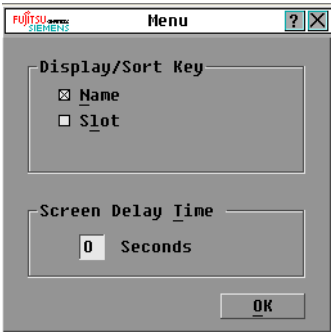

Figure 71: Menu Dialog Box

- Select **Slot** to display servers by slot number. Type a screen delay time of 1 second.
- Click **OK**.

3.2 Setting Up a BX600 Digital KVM Switch in Tiers

You can set up your BX600 Digital KVM Switch in tiers from our KVM appliances.

To connect the BX600 Digital KVM Switch to the supported KVM appliance:

NOTE: The supported KVM appliances can be: KVMs1-1602, KVMs2-0801, KVMs2-0411 or KVMs3-1621. Tiering is limited to 2 levels: Level 1 is the BX600 Digital KVM switch. Level 2 is any of the KVM appliances mentioned above.

- Place the BX600 blade chassis and the KVM appliance in the desired location. Fujitsu Siemens recommends powering off and unplugging both appliances before connecting them.
- Connect the keyboard, video, and mouse cable to the KVM appliance.
- Connect the other end of this cable to the Local KVM cable.
- Connect the Local KVM cable to the KVM port of the BX600 Digital KVM Switch (Figure 72).
- Connect the power cords for both the KVM appliance and the BX600 blade chassis to the appropriate socket on the back of the appliance.
- Connect both the KVM appliance and the BX600 blade chassis to an appropriate power supply.
- Turn the power on for the BX600 blade chassis first; then turn the power on for the KVM appliance.

NOTE: If the KVM appliance is powered on before the BX600 blade chassis, it may result in only 1 blade sever displaying in the KVM appliance interface instead of 10.

NOTE: In addition to the steps outlined above, some KVM appliances may require you to perform additional steps to ensure that the BX600 Digital KVM Switch blade servers appear in the KVM appliance interface. Please read your KVM appliance documentation for additional information.

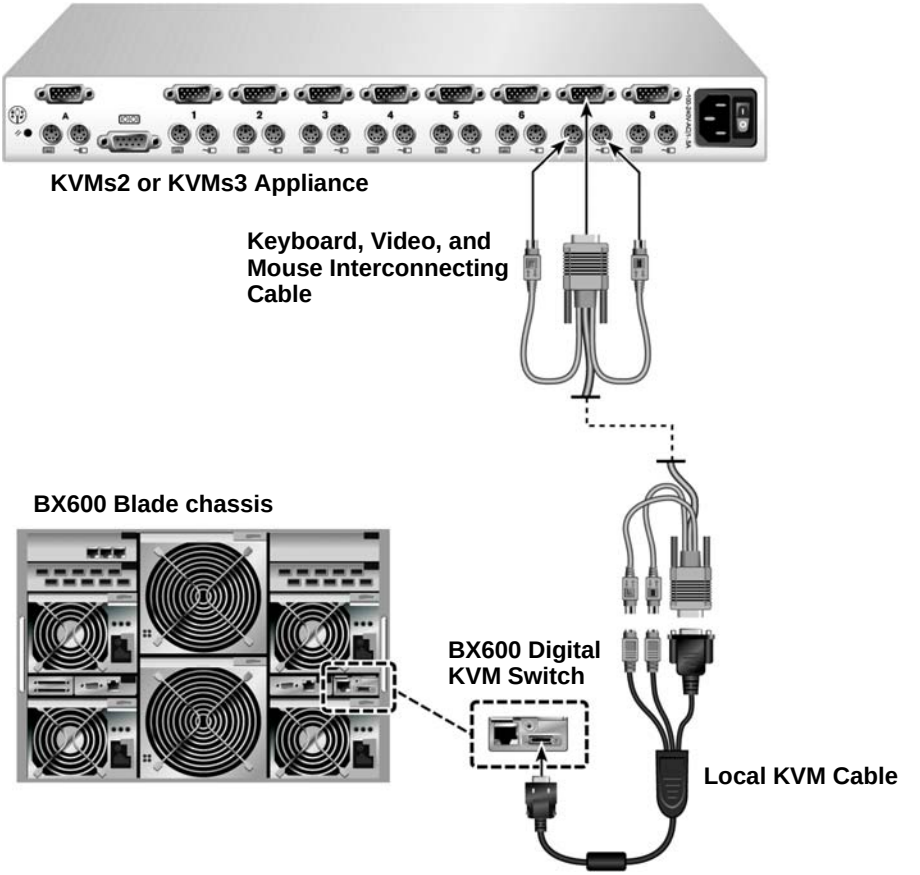
KVMs2 or KVMs3 Appliance
Keyboard, Video, and Mouse Interconnecting Cable
BX600 Blade chassis
BX600 Digital KVM Switch
Local KVM Cable

Figure 72: BX600 Digital KVM Switch tiered from a KVMs2-1602 or KVMs2-0801

Before connecting your BX600 Digital KVM Switch to a supported KVM appliance, you must ensure that it has been set to display in slot order and that the Screen Delay Time is set to 1 or more seconds. See “Analog Operation” on page 53. for more information. Once in slot order, it is possible for you also to set a Screen Delay Time that allows you to soft switch to a server without launching the OSCAR interface.

NOTE: Soft switching allows you to switch servers using a hot key sequence. You can soft switch to a server by pressing Print Screen and then typing the first few characters of its name or number. If you have a Delay Time set and you press the key sequences before that time has elapsed, the OSCAR interface will not display, allowing you more agility.

To configure the KVM appliance:

- Press Print Screen to open the OSCAR interface Main dialog box.
- Click **Setup** then click **Devices** and then click **Device Modify**.

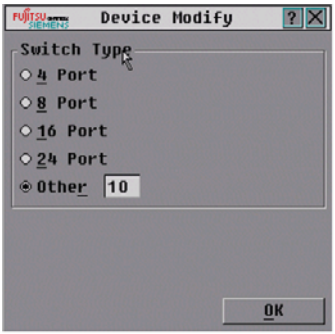

Figure 73: Device Modify Dialog Box

- Select the 10-port option to match the number of slots in the BX600 blade chassis. If the 10-port option is not available, select the 16-port option.
- Click **OK** to exit the OSCAR interface.
- Press Print Screen to verify that the settings have taken effect. The slot number of the blade to which the BX600 Digital KVM Switch is now attached should be expanded to display each of the slot locations of the servers in the BX600 blade chassis. For example, if the BX600 Digital KVM Switch is attached to slot 1, it would now be displayed as 01-01 to 01-10.

Figure 74: Main Dialog Box.

3.2.1 Tiering a BX600 Digital KVM Switch from a Console Switch

To tier a BX600 Digital KVM Switch from an Fujitsu Siemens s3-1621 Console Switch:

- Connect one end of a CAT5 cable to an ARI port on the Fujitsu Siemens s3-1621 Console Switch.

- Connect the other end of the CAT5 cable to a KVM Intelligent Adaptor (KVM-IA).
- Connect the local KVM cable to the local KVM port of the BX600 Digital KVM Switch and then to the KVM-IA.
- Once the BX600 Digital KVM Switch is connected, the server blades appear in the OSCAR interface.

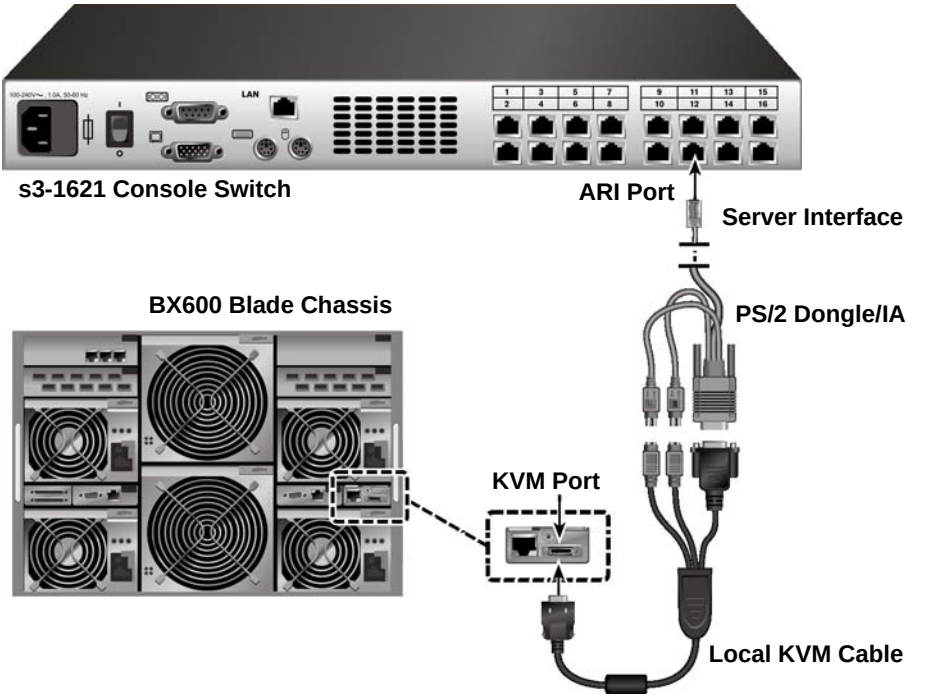

Figure 75: Tiering a BX600 Digital KVM Switch from an s3-1621 Console Switch

Once connected, the s3-1621 Console Switch will automatically configure the slots in the KVM menu. When the local system is set up, you will need to resynchronize the server list in the s3-1621 Console Switch software in order to see the list of BX600 blade chassis server blades. See your s3-1621 Console Switch documentation.

NOTE: With the KVMs3-1621 cascaded above the BX600 Digital KVM switch, you cannot attach virtual media via the KVMs3-1621 to the BX600 server blades.

4 Analog Operation

4.1 Controlling Your System

The BX600 Digital KVM Switch uses the intuitive menus of the OSCAR interface to allow you to select server modules and configure your system.

4.2 Viewing and Selecting Slots and Server Modules

Use the Main dialog box to view, configure, and control server modules connected to the BX600 Digital KVM Switch. You can view your server modules by name or by slot, but by default, you will see a Name list when you first launch the OSCAR interface.

To access the Main dialog box:

- Press Print Screen to launch the OSCAR interface. The Main dialog box appears.

  -or-

  If a password has been assigned, the Password dialog box appears. Type your password and click **OK**.
- The Main dialog box appears. For more information, see “Setting Console Security” on page 60.

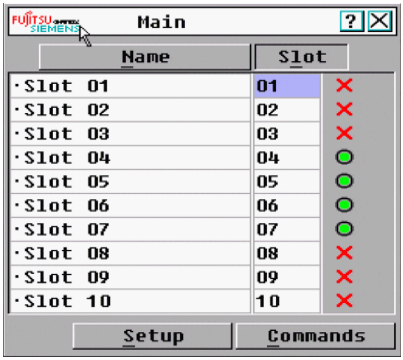

Figure 76: Example of Configured Main Dialog Box

NOTE: To launch the OSCAR interface, you can also press the Ctrl key twice within one second. You can use this key sequence in any place you see Print Screen throughout this User's Guide.

The OSCAR interface indicates the status of server modules in your system in the far right column of the Main dialog box. Table 1 describes the status symbols.

Symbol	Description
	Server Module is online
	PS/2 subsystem firmware is upgrading
	Server Module is offline or is not operating properly
	User connection

Table 1: OSCAR Interface Status Symbols

4.2.0.1 Selecting Server Modules

When you select a Server Module, the BX600 Digital KVM Switch reconfigures the keyboard and mouse to the proper settings for that Server Module.

To select server modules:

- Double-click the Server Module name or slot number.

  -or-

  If the display order of your Server Module list is by slot (Slot is depressed), type the slot number and press Enter.

  -or-

  If the display order of your Server Module list is by name (Name is depressed), type the first few letters of the name of the Server Module to establish it as unique, and press Enter twice.

To select the previous Server Module:

- Press Print Screen and then Backspace. This key combination toggles you between the previous and current connections.

To disconnect the analog user from a Server Module:

- Press Print Screen and then Alt + Ø. This leaves you in a free state, with no Server Module selected. The status flag on your desktop, if active, displays Free.

4.2.0.2 Soft Switching

Soft switching is the ability to switch server modules using a hot key sequence. You can soft switch to a Server Module by pressing Print Screen and then typing the first few characters of its name or number. If you have a Delay Time set and you press the key sequences before that time has elapsed, the OSCAR interface will not display.

To configure the OSCAR interface for soft switching:

- Press Print Screen to launch the OSCAR interface. The Main dialog box appears.

- Click **Setup** and then click **Menu**. The Menu dialog box appears.
- Select **Name** or **Slot** for the Display/Sort Key.
- For Delay Time, type the number of seconds of delay desired before the Main dialog box is displayed after Print Screen is pressed.
- Click **OK**.

To soft switch to a Server Module:

- To select a Server Module, press Print Screen. If the display order of your Server Module list is by slot as chosen above in step 3 (Slot is depressed), type the slot number and press Enter.

  -or-

  If the display order of your Server Module list is by name as chosen above in step 3 (Name is depressed), type the first few characters of the name of the Server Module to establish it as unique and press Enter.
- To switch back to the previous Server Module, press Print Screen then Backspace.

4.3 OSCAR Interface Navigation Basics

Table 2 describes how to use the keyboard and mouse to navigate the OSCAR interface.

Keystroke	Result
Print Screen or Ctrl	Opens the OSCAR interface. Press Print Screen twice (or Ctrl twice) to open the OSCAR interface on the currently selected device.
F1	Opens the Help screen for the current dialog box.
Escape	Closes the current dialog box without saving changes and returns to the previous one. In the Main dialog box, it closes the OSCAR interface and returns to the selected Server Module. In a message box, it closes the pop-up box and returns to the current dialog box.
Alt	Opens dialog boxes, selects or checks options and executes actions when used in combination with underlined letters or other designated characters.
Alt+X	Closes current dialog box and returns to the previous one.
Alt+O	Clicks **OK**, then returns to the previous dialog box.
Enter	Completes the switch operation in the Main dialog box and exits the OSCAR interface.

Table 2: Keyboard and Mouse Navigation

Keystroke	Result
Single-click Enter	In a text box, it selects the text for editing and enables the left-arrow and right-arrow keys to move the cursor. Press Enter again to quit the edit mode.
Print Screen, Backspace	Toggles back to previous selection if no other keystrokes have been typed.
Print Screen, Alt+Ø	Immediately disconnects the analog user from a Server Module; no Server Module is selected. Status flag displays Free. (This only applies to the Ø on the keyboard and not the keypad.)
Print Screen, Pause	Immediately turns on screen saver mode and prevents access to that particular console, if it is password protected.
Up/Down Arrows	Moves the cursor from line to line in lists.
Right/Left Arrows	When editing a text box, these keys move the cursor within the column.
Home/End	Moves the cursor to the top or bottom of a list.
Backspace	Erases characters in a text box.
Delete	Deletes characters in a text box.
Numbers	Type from the keyboard or keypad.
Caps Lock	Disabled. Use the Shift key to change case.

Table 2: Keyboard and Mouse Navigation (Continued)

4.4 Configuring the OSCAR Interface

You can configure your BX600 Digital KVM Switch from the Setup menu within the OSCAR interface. Click Names when initially setting up your BX600 Digital KVM Switch system to identify server modules by unique names. Select the other setup features to manage routine tasks for your server modules from the OSCAR interface menu.

To access the Setup menu:

- Press Print Screen to launch the OSCAR interface. The Main dialog box appears.
- Click **Setup**. The Setup dialog box appears.

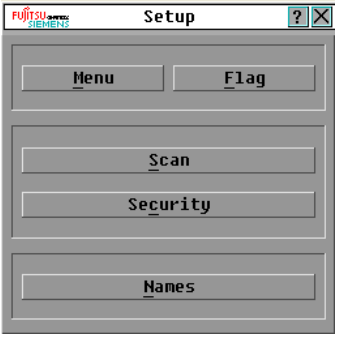

Figure 77: Setup Dialog Box

4.4.1 Assigning Server Module Names

Use the Names dialog box to identify server modules by name rather than by slot number. The Names list is always sorted by slot order.

To access the Names dialog box:

- Press Print Screen. The Main dialog box will appear.
- Click **Setup** and then click **Names**. The Names dialog box appears.

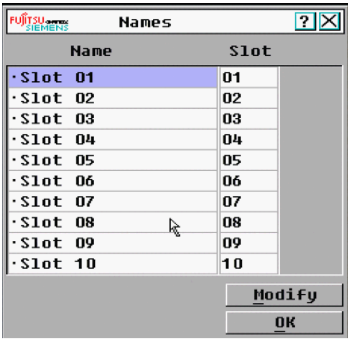

Figure 78: Names Dialog Box

NOTE: If the BX600 Digital KVM Switch System discovers new server modules, the on-screen list will automatically update. The mouse cursor will change into an hourglass during the update and the system will not accept mouse or keyboard input.

NOTE: The BX600 Digital KVM Switch stores the Server Module names. If you move a Server Module to a new slot or chassis, the name will not move with it, so the module must be reassigned a name in the new location.

To assign names to server modules:

- In the Names dialog box, select the name or slot number you wish to change and click **Modify**. The Name Modify dialog box appears.

Figure 79: Name Modify Dialog Box

- Type a name in the **New Name** field. Names of server modules may be up to 15 characters long. Allowable characters include: A-Z, a-z, Ø-9, space and hyphen.
- Click **OK** to transfer the new name to the Names dialog box. Your selection is not saved until you click OK in the Names dialog box.
- Repeat steps 1-3 for each Server Module in the system.
- Click **OK** in the Names dialog box to save your changes.

  -or-

  Click **X** or press Escape to exit the dialog box without saving changes.

4.4.2 Changing the Display Behavior

Use the Menu dialog box to change the display order of server modules and set a screen delay time for the OSCAR interface.

To access the Menu dialog box:

- Press Print Screen to launch the OSCAR interface. The Main dialog box appears.
- Click **Setup** and then click **Menu**. The Menu dialog box appears.

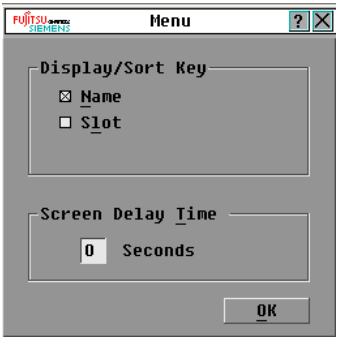

Figure 80: Menu Dialog Box

To choose the display order of server modules in the Main dialog box:

- Select **Name** to display server modules alphabetically by name.

-or-

Select **Slot** to display server modules numerically by slot number.

- Click **OK**.

To set a screen delay time for the OSCAR interface:

- Type in the number of seconds (Ø-9) you want to delay display of the OSCAR interface after you press Print Screen. Entering Ø will instantly launch the OSCAR interface with no delay.
- Click **OK**.

Setting a time to delay display of the OSCAR interface allows you to complete a soft switch without the OSCAR interface displaying. To perform a soft switch, see “Soft Switching” on page 54.

4.4.3 Controlling the Status Flag

The status flag displays on your desktop and shows the name of the selected Server Module or the status of a slot. Use the Flag dialog box to configure the flag to display by Server Module name, or to change the flag color, opacity, display time, and location on the desktop.

Flag	Description
Darrell	Flag type by name.
Free	Flag indicating that the user has been disconnected from all systems.

Table 3: OSCAR Interface Status Flags

To access the Flag dialog box:

- Press Print Screen. The Main dialog box will appear.
- Click **Setup** and then click **Flag**. The Flag dialog box appears.

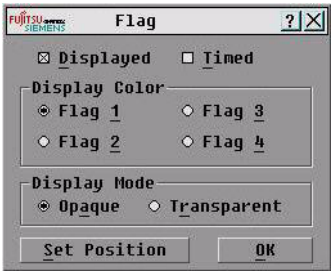

Figure 81: Flag Dialog Box

To determine how the status flag is displayed:

- Select **Displayed** to show the flag all the time or select **Displayed** and **Timed** to display the flag for only five seconds after switching.

NOTE: If only Timed is selected the flag will not be displayed at all.

- Select a flag color in Display Color. The flag numbers represent Flag 1, black; Flag 2, red, Flag 3, blue; and 4, purple.
- In Display mode, select **Opaque** for a solid color flag or select Transparent to see the desktop through the flag.
- To position the status flag on the desktop:
  a. Click **Set Position** to gain access to the Position Flag screen.
  b. Left-click on the title bar and drag to the desired location.
  c. Right-click to return to the Flag dialog box.

Figure 82: Position Flag

NOTE: Changes made to the flag position are not saved until you click OK in the Flag dialog box.

- Click **OK** to save settings.
  -or-
  Click **X** to exit without saving changes.

4.4.4 Setting Console Security

The OSCAR interface enables you to set security on your BX600 Digital KVM Switch console. You can establish a screen saver mode that engages after your console remains unused for a specified delay time. Once engaged, your console will remain locked until you press any key or move the mouse. You will then need to type in your password to continue.

Use the Security dialog box to lock your console with password protection, set or change your password, and enable the screen saver.

To access the Security dialog box:

- Press Print Screen. The Main dialog box will appear.
- Click **Setup** and then click **Security**. The Security dialog box appears.

NOTE: If a password has been previously set, the user will have to enter the password before being able to access the Security dialog box.

Figure 83: Security Dialog Box

To set or change the password:

CAUTION: There is no master password. The BX600 appliance must be sent to Fujitsu Siemens in the case of a lost password.

- Single-click and press Enter or double-click in the New text box.
- Type the new password in the New text box and press Enter. Passwords require 5 to 12 characters and must include at least one letter and one number. Passwords are also case sensitive. Legal characters are: A-Z, a-z, and 0-9.

NOTE: You can leave the New text box and the Repeat text box empty, if you do not want a password. (See "To remove password protection from your console:" on page 62.)

- In the Repeat box, type the password again and press Enter.
- Click **OK** if you only want to change your password, and then close the dialog box.

To password protect your console:

- Set your password as described in the previous procedure.
- Select **Enable Screen Saver**.
- Type the number of minutes for Inactivity Time (from 1 to 99) to delay activation of password protection and the screen saver feature.
- For Mode, select **Energy** if your monitor is ENERGY STAR™ compliant; otherwise select **Screen**.

CAUTION: Monitor damage can result from the use of Energy mode with monitors not compliant with ENERGY STAR™.

- (Optional) Click **Test** to activate the screen saver test which lasts 10 seconds then returns you to the Security dialog box.
- Click **OK**.

To log in to your console:

- Press Print Screen to launch the OSCAR interface. The Password dialog box appears.
- Type your password and then click **OK**.
- The Main dialog box appears if the password was entered properly.

To automatically log out of a Server Module when inactive:

- In the Main dialog box, click **Setup** and then click **Security**. If you have password protection, the Password dialog box appears.
- Type your password, and then click **OK**. The Security dialog box appears.
- In the **Inactivity Time** field, enter the length of time you want to stay connected to a Server Module before it automatically disengages you.
- Click **OK**.

To remove password protection from your console:

- In the Main dialog box, click **Setup** and then click **Security**. The Password dialog box appears.
- Type your password, and then click **OK**.
- In the Security dialog box, single-click and press Enter or double-click in the **New** field. Leave the box blank. Press Enter.
- Single-click and press Enter or double-click in the Repeat box. Leave the field blank. Press Enter.
- Click **OK** if you only want to eliminate your password.

To enable the screen saver mode with no password protection:

CAUTION: There is no master password. The BX600 appliance must be sent to Fujitsu Siemens in the case of a lost password.

- If your console does not require a password to gain access to the Security dialog box, continue to the next step.

  - or -

  If your console is password protected, see the previous procedure, *To remove password protection from your console:*
- Select **Enable Screen Saver**.
- Type the number of minutes for delay time (from 1 to 99) that you want to delay activation of the screen saver.
- Choose **Energy** if your monitor is ENERGY STAR™ compliant; otherwise select Screen.

CAUTION: Monitor damage can result from the use of Energy mode with monitors not compliant with ENERGY STAR™.

- (Optional) Click **Test** to activate the screen saver test which lasts 10 seconds then returns you to the Security dialog box.
- Click **OK**.

NOTE: Activation of the screen saver mode disconnects the user from a Server Module; no Server Module is selected. The status flag displays Free.

To exit the screen saver mode:

Press any key or move your mouse. The Main dialog box appears.

To turn off the screen saver:

- In the Security dialog box, clear **Enable Screen Saver**.
- Click **OK**.

To immediately turn on the screen saver:

- Press Print Screen, then press Pause.

NOTE: Enable Screen Saver must be selected in the Security dialog box.

4.5 Displaying Version Information

Use the Version dialog box to display the BX600 Digital KVM Switch firmware, hardware and FPGA versions, and to identify the language and keyboard configuration. For optimum performance, keep your firmware current. For more information on updates, see “OSCAR Interface Refresh Rates” on page 90.

To display version information:

- Press Print Screen. The Main dialog box will appear.
- Click **Commands** and then click **Display Versions**. The Version dialog box appears. The top half of the box lists the subsystem versions in the BX600 Digital KVM Switch.

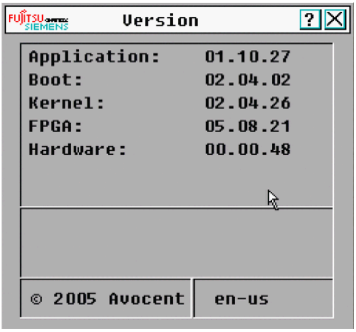

Figure 84: Version Dialog Box

- Click **X** or press Escape to close the Version dialog box.

4.6 Scanning Your System

In scan mode, the BX600 Digital KVM Switch automatically scans from slot to slot (Server Module to Server Module). You can scan up to 10 server modules by specifying which server modules you want to scan and the number of seconds that each Server Module will display.

To add server modules to the Scan list:

- If the OSCAR interface is not open, press Print Screen. The Main dialog box will appear.
- Click **Setup** and then click **Scan**. The Scan dialog box appears.

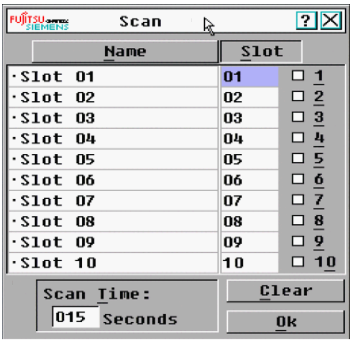

Figure 85: Scan Dialog Box

- The dialog box contains a listing of all the server modules attached to your unit. Click to enable the check box next to the server modules you wish to scan.

  -or-

  Double-click on a Server Module's name or slot.

  -or-

  Press Alt+ the number of the Server Module you wish to scan. You can select up to 10 server modules.
- In the **Scan Time** field, type the number of seconds (from 3 to 99) of desired time before the scan moves to the next Server Module in the sequence.
- Click **OK**.

To remove a Server Module from the Scan list:

- In the Scan dialog box, click to disable the check box next to a Server Module to be removed.

  -or-

  Double-click on a Server Module's name or slot.

  -or-

  Click **Clear** to remove all server modules from the Scan list
- Click **OK**.

To start the scan mode:

- Press Print Screen. The Main dialog box will appear.
- Click **Commands**. The Command dialog box appears.

Figure 86: Command Dialog Box

- 3 Select **Scan Enable** in the Command dialog box.

To cancel scan mode:

- Select a Server Module if the OSCAR interface is open.

  -or-

  Move the mouse or press any key on the keyboard if the OSCAR interface is not open. Scanning will stop at the currently selected Server Module.

  -or-

  Press Print Screen. The Main dialog box will appear.
- Click **Commands**. The Command dialog box appears.
- Clear **Scan Enable**.

5 Digital Operation

The BX600 Digital KVM Switch allows you to manage both blade servers and virtual media from a remote location. Using the Video Viewer, you can view and manage any of ten blade servers remotely in exactly the same way that you would if you were sitting in front of them. Using the Virtual Media dialog box, you can manage virtual media sessions allowing you to remotely perform server backups, recovery operations, and operating system installation to name a few examples. For each of these operations, you go through the Fujitsu Siemens Management Blade (MMB).

Your client machine must meet minimum requirements to access the MMB, the video viewer or manipulate virtual media (See Appendix B).

5.1 Accessing BX600 Digital KVM Switch through Fujitsu Siemens (MMB)

Point your browser to the IP address of the MMB to access the BX600 Digital KVM Switch. You may then access the video viewer and manipulate virtual media.

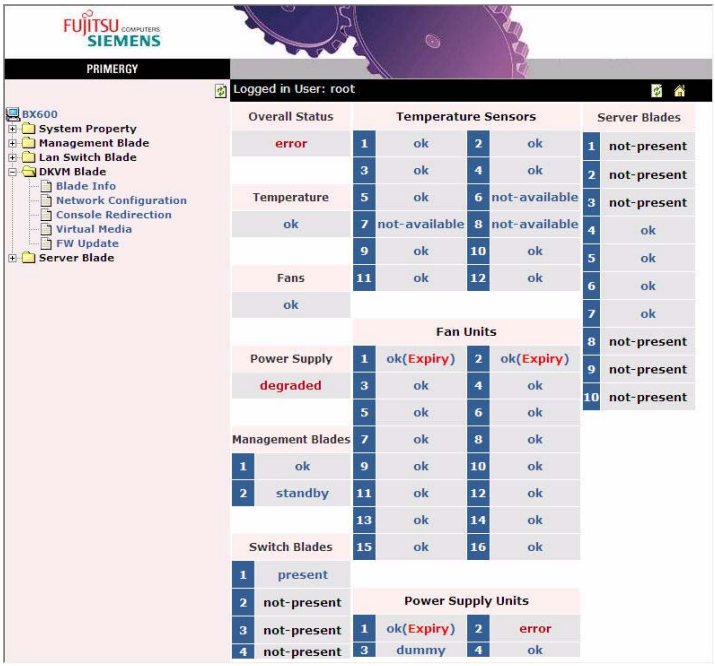

Figure 87: Fujitsu Siemens Management Blade (MMB) Home Page

To access the Video Viewer application:

- From your browser, type in the correct URL to bring up the MMB interface.
- Click on the plus sign (+) next to the **DKVM** folder in the left column to display the folder's contents.

- On the left side, select **Console Redirection**.
- On the right side, select the Server Blade from the drop-down list.
- Click on **Launch**.

5.2 Using the Video Viewer

Once you have selected Console in the MMB menu, you may select the server you would like to interact with.

To access a server:

- Click the **Servers** button in the list of servers.
- Click the **Select Server** button. The Launch Application button will become active.
- Click the **Launch Application** button. The server's desktop will appear.

5.2.1 Interacting With the Server Being Viewed

Once you have connected to a server, a separate desktop window of the server will appear on your screen. You will see two cursors: the local cursor and the server's cursor. You may need to align these if they do not move together or adjust the video if they seem to jump about. From this window, you will be able to access all the normal functions of this server as if you were sitting right in front of it. You may also perform Viewer-specific tasks such as sending special Macro commands to the server.

The Video Viewer synchronizes the remote and local mouse pointers every time the remote mouse pointer enters the Video Viewer's video window. Synchronization is accomplished by sending a 'Mouse Align' message to the BX600 Digital KVM switch every time the mouse cursor enters Video Viewer's video window.

NOTE: The BX600 Digital KVM switch screen resolution must be equal to or larger than the server screen resolution.

5.2.1.1 Server Name Modifications

The Server Module names may be assigned using the Web GUI interfaces as well as the OSCAR interface.

To change a server module name using the Web GUI interface:

- Point your browser to the IP address of the MMB to access the BX600 Digital KVM Switch.
- Left-click your mouse on the **plus sign** next to the **Server Blade** folder icon.
- Left-click the **plus sign** next to the Server Blade whose name you want to change.
- Left-click the **plus sign** next to **Blade Info**. You should see a web page similar to the one displayed Figure 88.

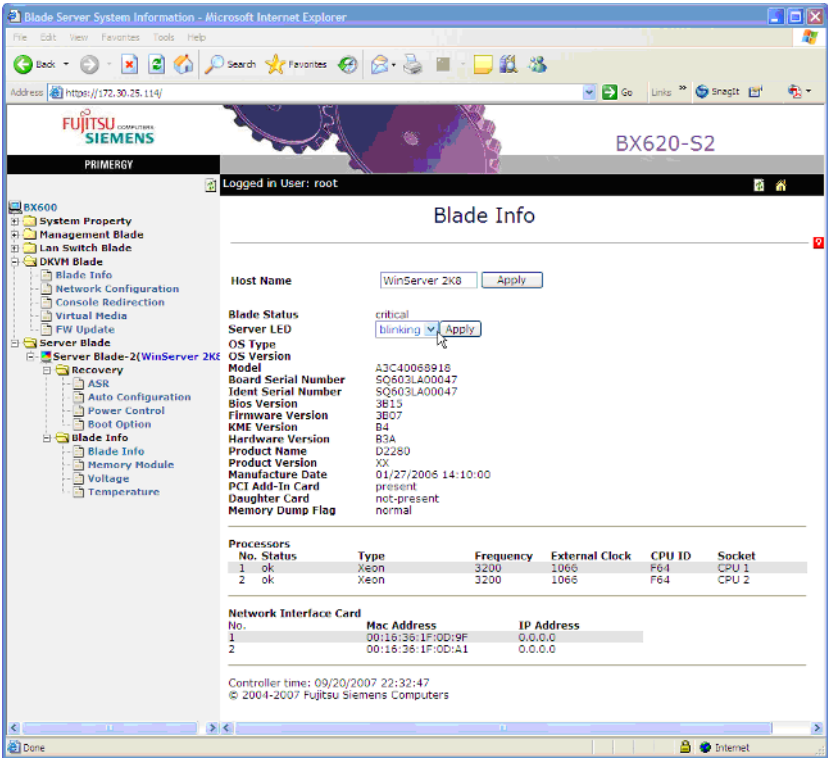

Figure 88: Blade Info Page

To change the Server Blade module name:

- Click on the **Host Name** field and enter the new host name in the field.
- Click on the **Apply** button to update the Server Blade module name. In this example, the Server Blade module name for the blade server installed in slot 2 has been changed to “WinServer 2K8”.

  Server Module names modified via the Web GUI are transferred to and displayed on OSCAR. The maximum length of a server name in OSCAR is 15 characters plus a null terminator. Names exceeding 15 characters will be truncated when viewed in OSCAR. In this example, the OSCAR display would look similar to the following figure.

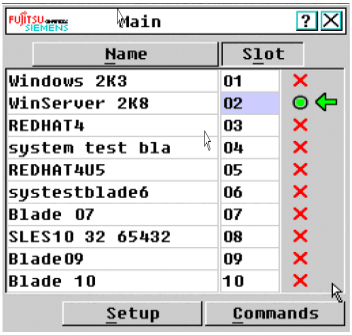

Figure 89: Server Module Names in OSCAR

5.2.1.2 Video Viewer command panel

A command panel is displayed at the bottom of the Video Viewer window. A command panel example is shown in the following figure.

Figure 90: Video Viewer Command Panel

There is a Blade Selection drop-down menu in the command panel of Video Viewer to select the blade being viewed. The drop-down menu displays a list of the available blades. Each blade is referenced by its name. The names will appear in their positional order (i.e. Blade 1 will be first, Blade 2 second and so on). Preceding each name will be the slot number followed by a hyphen. The slot numbers will be single digits for slot numbers less than 10. To select a blade for viewing the user need only click on the drop-down menu's down arrow and then click on the desired blade's name.

The keystroke prefixes Ctrl, Alt and SysRq can be passed to the target server of the Video Viewer by selecting one or more of the **Crtl**, **Alt** or **SysRq** checkboxes in the command panel. Any time any of the Keystroke Prefix checkboxes are selected, they will be subsequently cleared when another key is pressed.

If the blade being viewed in the Video Viewer changes for any reason, then the name of the server being viewed on the caption bar of the Video Viewer shall change to indicate the name of the newly selected server being viewed.

5.2.1.3 KVM Session Premption

The BX600 Digital KVM web interface provides a method for notifying a remote KVM session user that another user would like to preempt their session.

To request preemption of the current user's KVM session:

- From the MMB home page, click **DKVM Blade** - **Console Redirection**. The KVM Console Redirection web page will appear.
- Click the **Preempt Session** button on the KVM Console Redirection web page, as shown in the following figure.

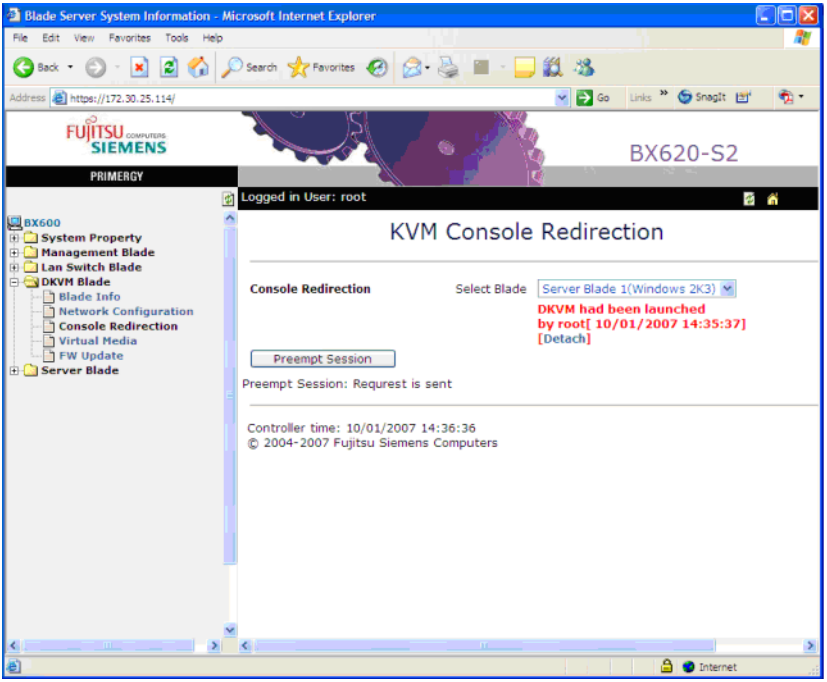

Figure 91: Preempt Session in Console Redirection Screen

5.2.1.4 Current user response to preemption request

The current user will be shown a Session Preemption Request dialog box, indicating that another user (your user name will be indicated) would like to preempt the current session.

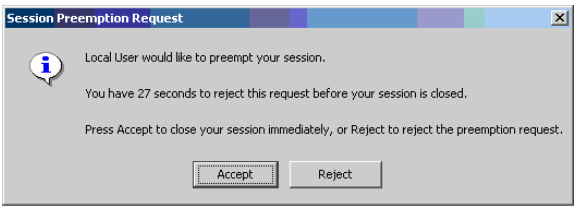
Session Preemption Request
Local User would like to preempt your session.
You have 27 seconds to reject this request before your session is closed.
Press Accept to close your session immediately, or Reject to reject the preemption request.
Accept
Reject

Figure 92: Preemption Request Dialog Box

The current user shall have the chance to:

- Respond with an acceptance of the preemption, which will occur immediately.
- Respond with an acceptance of the premption with a specified time delay.
- Reject the preemption.

NOTE: The preemption notice in the Video Viewer shall be non-modal so that the user may still interact with the remote KVM session while the preemption notice is displayed.

- Ignore the preemption request, which will cause the preemption notice shall time out after 30 seconds. If the current user has not responded within that period, then

the Video Viewer assumes that the user is not present and that the remote KVM session may be preempted immediately.

The **Accept** button allows the current user to accept the preemption. When the current user presses the button, the dialog box will change to the drop-down dialog box shown in Figure 93, and the current user can select a time delay from 0 to 20 minutes. You will be notified of the current user's response and the time delay. The caption bar of the Video Viewer will display the number of seconds remaining until closure.

The drop-down dialog-box of the Session Preemption dialog displays the number of minutes until the user will close the remote session. Available entries in the drop-down list are: 0, 1, 2, 3, 4, 5, 10, 15 and 20 minutes. The default value selected in the drop-down will be 5 minutes as shown in Figure 93.

After the time the current user specifies has elapsed, the remote console session shall close and a preemption response command will be sent to the BX600 Digital KVM indicating that the current user has accepted the preemption request and that the number of seconds until the user closes the session is zero (i.e. the remote session has closed).

The **Reject** button allows the user to reject the preemption. When the user presses the button the dialog shall close and a preemption response message shall be sent to the BX600 Digital KVM indicating that the current user has rejected the preemption request.

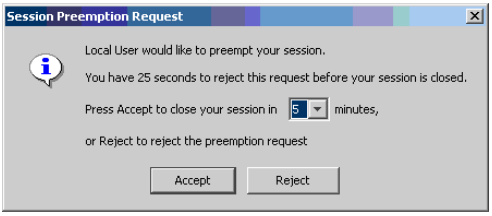
Session Preemption Request
Local User would like to preempt your session.
You have 25 seconds to reject this request before your session is closed.
Press Accept to close your session in
5
minutes,
or Reject to reject the preemption request
Accept
Reject

Figure 93: Preemption Request Countdown Dialog Box

5.2.2 Viewer Window Features

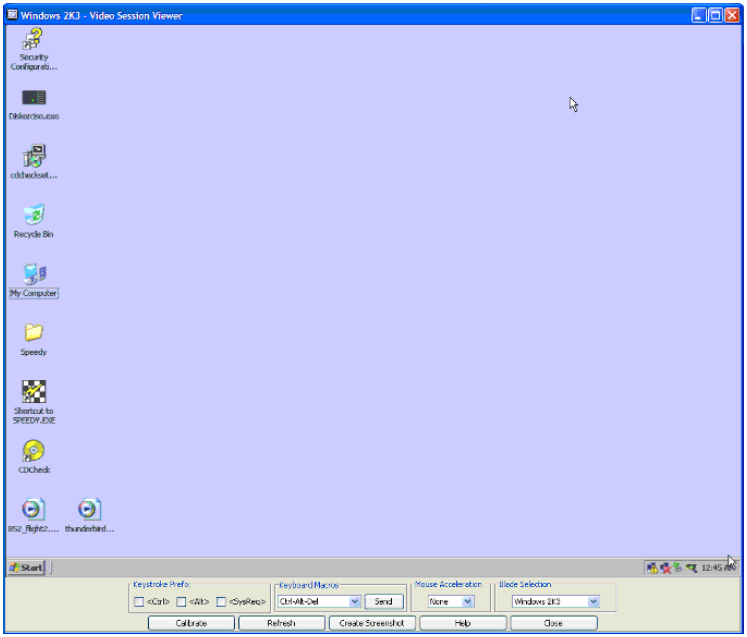

Figure 94: Video Viewer Application

5.2.3 Expanding and Refreshing Your Viewer

You can adjust your view of the remote system's monitor using the buttons at the bottom of the Viewer window. The buttons allow you to set video adjustments, refresh the screen, capture screen images, get help and close the Video Viewer application. There are also some check boxes and drop-down lists that let you pass special keystrokes to the remote system without affecting your local workstation.

To set video adjustments:

- Click **Calibrate** on the viewer toolbar.

  This automatically calibrates and sets the video adjustments. You also have the option to launch a manual video adjustment dialog box. See "Manual Video Adjust Dialog Box Options" on page 75.

To refresh the screen image in the Video Viewer:

- Click **Refresh** on the viewer toolbar.

To capture a screen image from the Video Viewer:

- Click **Create Screenshot** on the viewer toolbar.

To get help:

- Click **Help** on the viewer toolbar.

To close the Video Viewer application:

- Click **Close** on the viewer toolbar.

5.2.4 Adjusting the Viewer Window

- You can adjust both the size and quality of the server's Viewer. You can also expand your Viewer to fit the entire screen or refresh the view at any time.

5.2.5 Adjusting Keyboard Macros

- Allows you to select and type a number of keystroke combinations that cannot be typed using your local keyboard without affecting your local system.

To use any one of the keystroke combinations listed:

- From the Keystroke Macros list, select the macro you want to send.
- Click **Send**. The keystroke macro is sent to the remote system.

5.2.6 Setting a Keystroke Prefix

- Click to enable one or more of the Keystroke Prefix check boxes to enable you to select a key or key combination that acts as a previous keystroke to your actual keystrokes.

5.2.7 Adjusting Mouse Acceleration

The Mouse Acceleration list allows you to select the operating system you want to view. Select the appropriate operating system to optimize console redirection mouse performance. You can select **None** for Windows and most other operating systems and **Linux** for the Linux operating system.

5.2.8 Adjusting the Video Quality

The Viewer offers both automatic and manual video adjustment capability. Generally, the Automatic Video Adjustment will optimize the video for the best possible view. However, you may wish to alter the video for your specific needs. Use the slider bar for fine adjustments, and the Plus (+) and Minus (-) buttons for small, incremental adjustments.

NOTE: Only 7-bit color is supported.

5.2.9 Manual Video Adjust Dialog Box Options

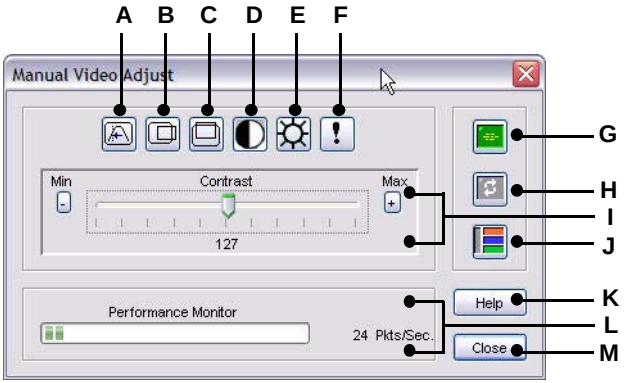

Figure 95: Manual Video Adjust Dialog Box

A Pixel Sampling Fine Adjustment
B Image Capture Horizontal Position
C Image Capture Vertical Position
D Contrast
E Brightness
F Pixel Noise Threshold
G Automatic Video Adjustment
H Refresh Image
I Scroll Bar (for active button)
J Three Color Video Test Pattern
K Help Button
L Performance Monitor
M Close Button

To manually adjust the video quality of the Viewer window:

- In the Viewer, click **Calibrate**. The Auto Video Adjust dialog box appears.
- Click the **Manual Video Adjust** button.
- Click the icon for the feature you wish to adjust.
- Move the slider bar or click Minus (-) or Plus (+) to adjust the parameter one unit at a time for each icon pressed. The adjustments will display immediately in the Viewer window.
- When finished, click **Close** to exit the Manual Video Adjust dialog box.

5.2.10 Minimizing Remote Video Session Discoloration

When establishing remote video sessions, pixel discolorations may occur due to network conditions. This condition occurs most often with a solid color background. This

condition is minimized by using a black background. If a color background is used, a small number of pixels on the screen will be discolored or white.

To minimize remote video pixel discoloration:

- In the Viewer, click **Calibrate**. The Auto Video Adjust dialog box appears.
- Click the **Manual Video Adjust** button.
- Choose contrast or brightness.
- Adjust the contrast and brightness until the image quality improves.
- A noise threshold setting is also available and then **Manual Video Adjust** for fine incremental adjustments.

NOTE: Reducing the noise threshold to zero causes constant video refresh, high network usage and a flickering video. Fujitsu Siemens recommends that the noise threshold be set to the highest level that allows efficient system performance, while still being able to recover pixel colors over which the mouse cursor travels.

NOTE: When adjusting the noise threshold, use the slider bar for large adjustments and Plus (+) and Minus (-) at the ends of the slider bar for fine-tuning.

5.2.11 Improving Screen Background Color Display

You may experience inconsistent color display when viewing target servers where photographic images or color-intense gradient backgrounds have been selected. We recommend that you select a solid color display background via the operating system for optimal display quality and performance.

- Use the Plus (+) and Minus (-) buttons at the end of the slider bar to fine-adjust the noise threshold to just above zero.

NOTE: Leaving the noise threshold at zero triggers constant video refresh, resulting in high network usage and a flickering video. It is recommended that the noise threshold be set at the highest level that allows efficient system performance, while still being able to recover pixel colors that the mouse cursor travels over.

NOTE: When adjusting the noise threshold, the slider bar can be used for large or very fine adjustments and the Plus (+) and Minus (-) buttons at either end of the slider bar for small, incremental adjustments.

5.2.12 Improving Mouse Performance

If you are experiencing slow mouse response during a remote video session, you may want to deactivate the mouse acceleration in the operating system of the target server.

Microsoft Windows XP Default Mouse Drivers:

- Select **Start** then select **Settings** and then select **Control Panel**.
- Double-click the Mouse icon.
- Click on the **Motion** tab.
- Adjust mouse speed to the exact midpoint of the slider bar.
- In the Acceleration setting, select the **Off** radio button.
- Click **OK**. Click Mouse Synchronize/Screen Refresh in Video Session Viewer to resynchronize the mouse.

Intellipoint Drivers (Only for Windows based Operating Systems):

- Select **Start** then select **Settings** and then select **Control Panel**.
- Double-click the Mouse icon.
- Cycle through the tabs until the pointer speed slider is displayed.
- Adjust the mouse speed to the exact midpoint of the slider bar.
- Click **Advanced**.
- Click the **Acceleration** check box to turn off acceleration.
- Click **OK**. Click **Mouse Synchronize/Screen Refresh** in Video Session Viewer to resynchronize the mouse.

Red Hat Linux:

- Select the **Mouse** settings from the Desktop Controls.
- Set Acceleration to 1.0.
- Apply the changes and click **Mouse Synchronize/Screen Refresh** in Video Session Viewer to resynchronize the mouse.

Any Linux Distribution:

- Open a Console window in the Desktop.
- Enter the following command:

```
xset m 0
```

NOTE: On some Linux distributions, this procedure needs to be performed each time you log onto the Desktop.

5.2.13 Create Screenshot Images

The **Create Screenshot** button captures the current remote system screen to a .jpg file on the local system. A dialog box is displayed that allows you to save the .jpg file to a specified location.

5.3 Virtual Media

5.3.1 Virtual Media Dialog Box

The Virtual Media dialog box allows you to map a single generic mass storage device (or floppy image) and a single CD/DVD device (or CD/DVD image) to a target server. Once you have selected Virtual in the MMB menu, you may select the server you would like to interact with.

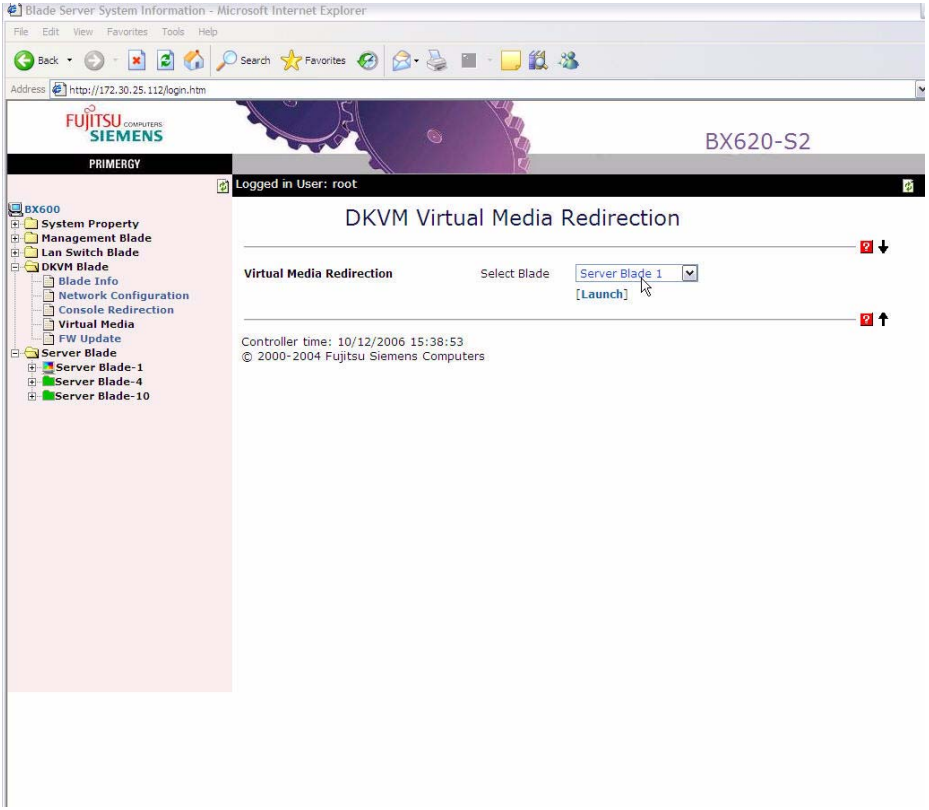

Figure 96: Virtual Media page of the MMB menu

To access a server:

- Click the **Select Blade** drop-down list in the list of servers.
- Select the server on which you want to attach your virtual media. The launch button will become active.
- Click the **Launch** button. The Virtual Media dialog box will appear. It will be associated with the server you chose from the drop-down list.

5.3.1.1 Mapping a Floppy Device

The Floppy Drive panel allows you to select a floppy drive from a list of all client floppy drives. You can also select the Floppy Image option that allows you to browse to the location of your chosen floppy image file. If you do not want to select either of these options you can select the None option.

NOTE: Only one Generic Mass Storage Devices or Filesystems option can be selected at any one time. The selected generic mass storage device is not mapped until you click Connect Floppy.

5.3.1.2 Mapping a CD/DVD Device

The CD/DVD Drive panel allows you to select a CD/DVD device from the attached CD/DVD drives. You can also select the ISO Image option to select a single CD/DVD image file. If you do not want to select either of these options you can select the None option.

NOTE: Only one CD/DVD Devices or Filesystem option can be selected at any one time. The selected generic mass storage device is not mapped until you click Connect CD/DVD.

5.3.1.3 Viewing the Mapped Device Status

The Status panel lists the generic mass storage device and CD/DVD device that are currently mapped. For each mapped device, the target drive, where the target drive is mapped and the number of bytes read (for that device) are displayed.

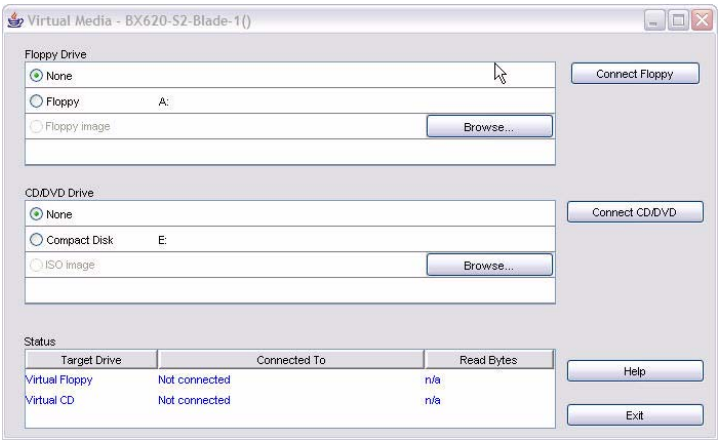

Figure 97: Virtual Media Dialog Box

6 BX600 Graphical User Interface

The Fujitsu Siemens BX600 Digital KVM Switch allows you to access the blades in a BX600 Blade Server using a Graphical User Interface (GUI).

To access the Fujitsu Siemens Management Blade (MMB) GUI:

- Point your browser to the IP address of the MMB to access the BX600 Digital KVM Switch.

When the Fujitsu Siemens Management Blade GUI is called up, the first screen that appears has a list of folders in the left hand column that consist of the following:

- System Property
- Management Blade
- Lan Switch Blade
- DKVM Blade
- Server Blade

6.1 DKVM Blade Folder Contents

The scope of this chapter will discuss the DKVM Blade folder, its contents and how to perform the various tasks.

To access the DKVM Blade folder pages:

- Click the plus sign (+) next to the DCVM folder icon in the left column of the GUI screen.

The DKVM Blade folder contains the following pages:

- Blade Info
- Network Configuration
- Console Redirection
- Virtual Media
- Firmware Update

6.2 Blade Info

Blade Info is a page in the folder that displays the information about the BX600 Digital KVM switch that is installed in the BX600 blade server.

To access the Blade Info page:

- Select **Blade Info** from inside the **DKVM Blade** folder in the left column.

When this page is selected, the BX600 reads the blade information from the BX600 Digital KVM switch. This page shows the following items:

- DKVM blade Manufacture
- DKVM blade Manufacture Date
- DKVM blade Serial Number
- DKVM blade Product Name
- DKVM blade Model Name

- DKVM blade Hardware Version

6.3 Network Configuration

In order for you to have GUI access to the BX600 Digital KVM switch, you must assign a valid IP address to it.

NOTE: If your local area network is configured for DHCP, you should check the **DHCP** check box and you can skip the first three steps of the following task.

To configure the BX600 Digital KVM switch with an IP address:

- Select **Network Configuration** from inside the **DKVM Blade** folder in the left column.
- Assign an IP address to the BX600 Digital KVM switch by filling in the boxes in the **KVM IP Address** field.

NOTE: The IP address of the BX600 Digital KVM switch must be in the same subnet as the Fujitsu Siemens BX600 Management Blade Module.

- Enter the default gateway address by filling in the boxes in the **Default Gateway** field.
- Enter the network mask by filling in the boxes in the **Network Mask** field.
- If necessary, enter a port address in the **Keyboard/Mouse Port** field. In most cases, you can leave this setting at the default value.
- If necessary, enter a port address in the **Virtual Media Port** field. In most cases you may leave this setting at the default value.
- If necessary, enter a port address in the Video Port field. In most cases you may leave this setting at the default value.
- Click on **Apply Changes**.

A typical network configuration page is shown in the following illustration.

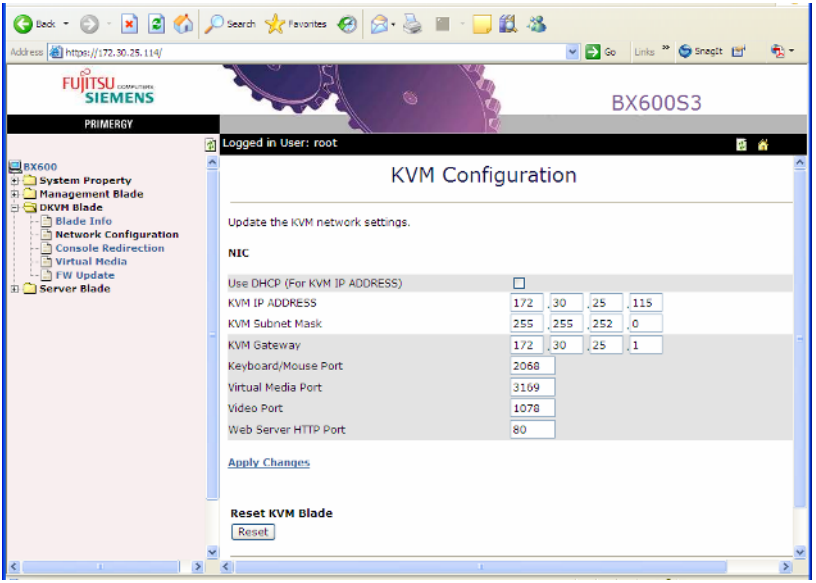

Figure 98: DKVM Network Configuration Page of the MMB Menu

6.4 Console Redirection

The Console Redirection page is the page that you use to launch the Video Viewer application.

To redirect the console to a Video Viewer of your selected blade server:

- Select **Console Redirection** from inside the **DKVM Blade** folder in the left column.
- Select a blade server from the drop-down list in the screen that appears.
- Click on **Launch**.

The Console Redirection page is shown in the following illustration.

Figure 99: Console Redirection Page of the MMB Menu

For details on using the Video Viewer, see “Using the Video Viewer” on page 68.

6.5 Virtual Media

The BX600 Digital KVM switch allows you to use media on your local workstation as if it were installed on the remote blade server. This feature is known as virtual media.

To launch the Virtual Media Dialog Box:

- Select **Virtual Media** from inside the **DKVM Blade** folder in the left column.
- Select a blade server from the drop-down list in the screen that appears.
- Click on **Launch**.

For details on using Virtual Media, see “Virtual Media” on page 77.

6.6 FW Update

You can update the firmware on the BX600 Digital KVM switch from the MMB.

To update BX600 Digital KVM firmware:

- Select **Firmware Update** from inside the **DKVM Blade** folder in the left column.
- Enter the file name in the **Image Name** field that appears in the right portion of the MMB page.
- Enter the IP address of the TFTP server where the firmware resides by filling in the boxes in the **TFTP Server IP** field.
- Click on **Update Firmware**.
- Optionally, you may click on **Firmware Update Status** to see how the firmware update is progressing.

CAUTION: Never interrupt a firmware update in progress. It can make your BX600 Digital KVM switch inoperable, and it will be necessary to return it to Fujitsu Siemens for a firmware reinstallation.

The Firmware Update page is shown in the following illustration.

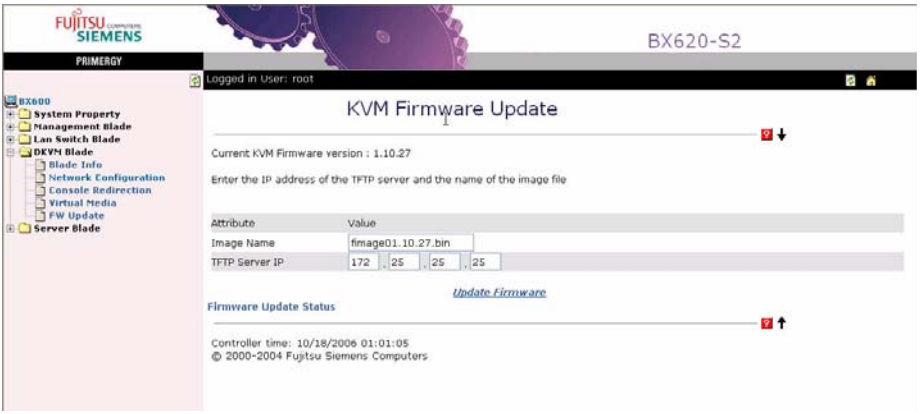

Figure 100: Firmware Update Page of the MMB Menu

7 Appendices

7.1 FAQs (Frequently Asked Questions)

Q: What is the OSCAR interface?

A: The OSCAR interface (On-Screen Configuration and Activity Reporting interface) is a utility that allows you to configure and manage the integrated KVM switch. The OSCAR interface provides intuitive menus that allow you to configure your system, and select computers.

Q: How do I connect to the OSCAR interface?

A: Connect a monitor, a PS/2 keyboard, and a mouse to the analog port on the back of the Digital Access KVM switch. Once connected, to invoke the OSCAR interface:

- Press <Print Screen>.

  -or-
- Press <Ctrl> twice.

  -or-
- If a password has been assigned, the **Password** dialog box appears. Type your password and click **OK**. The **Main** dialog box appears.

Q: What is soft switching?

A: Soft switching is the ability to switch servers using a hot key sequence. You can soft switch to a server by pressing <Print Screen> and then typing the first few characters of its name or number.

Q: What do the OSCAR interface status indicators mean?

A: The status to the right of the slot number in the **Main** dialog box of the OSCAR interface indicates the status of the server.

Indicator	Status
	Green light - blade server module is currently online
	Red “X” - blade server is currently offline
	Green arrow - user connection to switch
	Yellow light - PS/2 subsystem firmware is upgrading

Table 4: OSCAR Interface Status Symbols

Q: How do I set the position of the OSCAR interface status flag?

A: To position the status flag:

- In the OSCAR interface Flag dialog box, click **Set Position**.
- Click and drag the title bar to the desired position.
- Right-click to return to the Flag dialog box.

Q: If I power down a blade, will it still be scanned?

A: No, only servers that are powered up are scanned. If a server is powered down it will be skipped during a scan.

Q: Can I set a password on the OSCAR interface?

A: Yes. In the **Security** dialog you can set a screen saver password that must be entered to access the OSCAR interface once the screen saver has activated. In the **Security** dialog you can also choose to enable or disable the screen saver and enter the duration for which the keyboard and mouse must be inactive before **Screen Saver** mode is activated.

Q: Can I assign names to individual blades in the OSCAR interface?

A: Yes. The **Names** dialog box allows you to assign names to blade servers. By default all servers are given the name **Slot** followed by a number signifying the order in which were brought online.

NOTE: Naming information is not retained in the blade server. Therefore, each time a blade is moved and configured in a new server; it must be assigned a name in the **Names** dialog box.

Q: How do I scan servers in the OSCAR interface?

A: The **Scan** dialog box allows you to select a list of servers to scan while the OSCAR interface is in scan mode, and also to set the time period for which each server is displayed. To begin a scan of the servers in your scan list, you must enable the **Scan** check box in the **Commands** dialog box.

Q: Can I interact with a server while in scan mode?

A: No. While in scan mode, you can view servers but cannot control the keyboard and mouse until the scan has completed.

Q: How do I view the Application firmware version number?

A: You can view all version information for the KVM switch in the **Version** dialog box**.** To access the **Version** dialog box:

- In the **Main** dialog box, click **Commands.** The **Commands** dialog box appears.
- Click **Display Versions**. The **Version** dialog box appears.

Q: How do I access the Application firmware build version number?

A: All three-part version numbers consist of the major version number, the minor version number and the development version number. The fourth part, the build version number is hidden from this screen. A special key sequence is required to display the four part version numbers on this screen. When you press <Print Screen>, or <Ctrl><Ctrl> to display the OSCAR interface, immediately followed by a <CTRL><V>, the four-part version numbers is displayed.

Q: Can I connect my USB keyboard and mouse to the integrated KVM switch?

A: No, only a PS/2 keyboard and mouse can be connected to the integrated KVM switch.

Q: I am having difficulty viewing the OSCAR interface using my VGA monitor?

A: Verify that your monitor is compatible with the Digital Access specifications and that it is correctly configured. The maximum allowable resolution is 1600 X 1200 at 80 Hz. Please consult the *Digital Access User's Guide* for further details.

Q: How do I upgrade integrated KVM switch firmware?

A: The integrated KVM switch's firmware is upgradeable through the Fujitsu Siemens Management Blade (MMB). Please consult the Primergy BX600 User's Guide for details on firmware upgrades.

Q: How do I remotely access the KVM switch?

A: All access to the KVM switch is obtained via the MMB. Point your browser to the IP address of the MMB to get the GUI for the MMB. Click on the 'MMB' menu on the left side of the GUI to open the pull-down menu beneath it. At this point, you may open the Video Viewer by selecting **Console**, or work with Virtual Media by selecting **Media**.

Q: How does one manage the individual blade servers?

A: The BX600 Digital Access KVM Switch Module allows you to manage both blade servers and virtual media from a remote location. Using the Video Viewer, you can view and manage servers remotely as if you were physically present. Once you have selected **Console**, you may select the server you would like.

- From the list of servers, click the button that represents the server you would like to view
- Click the **Select Server** button at the bottom of the display. When the system has successfully made the selection, the Launch Application button will become active.
- Click the **Launch Application** button. The server's desktop will appear.

Q: How do I synchronize the movements of the mouse on my management station with the mouse movements associated with my target blade server?

A: As you move the client's cursor, the remote server's cursor will shadow it closely, in both movement and position. You may need to align these if they do not move together. Additionally, you may need to adjust the video if the cursors seem to jump erratically. To align the mouse cursors:

Click the menu beneath the **Mouse Acceleration** and then choose the closest match to your client operating system from the menu. The system will automatically realign the cursors.

NOTE: It may be necessary to adjust the mouse properties for the particular OS of your target server. Typically for Windows Server OSs, you may need to adjust the Pointer Options of the Mouse Motion Properties by unchecking the box for *Enhance pointer precision*. For Linux, open a terminal window and type: *xset m 0* (zero) and press Enter.

Q: What is Virtual Media and how is it implemented?

A: Often an IT administrator will not only need remote KVM control of blade servers, but also the ability to remotely load software on the system. To accommodate this

requirement, the Digital Access KVM module supports “virtual” connections to remote USB devices such as a CDROM/DVD, floppy drive, or USB flash drive. This ‘virtual’ connection from the local management station’s device to the remote server is known by the term “Virtual Media.”

Virtual Media allows you to map a single generic mass storage device (or floppy image) **AND** a single CD/DVD device (CD/DVD image) to a target server. When you have mapped a device, you will be able to see it from the remote console through the video viewer. You may then operate the device normally through the Video Viewer session. The device will behave as if it is physically attached to it.

Q: Which operating systems are supported on the management client station?

A: Operating systems supported on the management client station:

Windows XP, SP1 or SP2

Windows 2000 Server SP4, Windows 2000 Advanced Server SP4

Windows 2003 Server (Standard, Enterprise, Web Editions w/ SP1) (Internet Explorer enhanced security turned “off”)

Red Hat 3 WS,ES,AS

Red Hat 4 WS,ES,AS

Q: Which operating systems are supported on the blades?

A: Operating systems supported on the blades (BIOS version A04):

Windows 2000 Server, SP4

Windows 2000 Advanced Server, SP4

Windows 2003 Server (Standard, Enterprise, Web Editions) SP1 (required for virtual media)

Windows 2003 Server (Enterprise x64, Web x64 Editions) SP1 (required for virtual media)

Red Hat Enterprise Linux 3.0 (ES update 3 or later & AS update 3 or later)

Red Hat Enterprise Linux 4.0 (ES & AS)

Red Hat Enterprise Linux 4.0 x64 (ES & AS)

Q: What versions of Browsers are supported?

A: Supported browsers:

Internet Explorer 6.0 SP1 or SP2, or Internet Explorer 7.x

Mozilla 1.6.x or 1.7.3

Q: What versions of Java are supported?

A: Supported Java versions are JRE 1.4.2 or above

Q: What should be done in case of a Viewer/Display Resolution Mismatch when using Linux?

A: Switch to a Linux terminal window using Ctrl+Alt+F2 or Ctrl+Alt+F3... Ctrl+Alt+F6. Edit the file, */etc/X11/xorg.conf* and go to the section, *Screen* and set mode to 1024 x 768. Then restart the Xserver.

7.2 Technical Specifications

Server Module Slots	
Number	10
Plug and Play	DDC2B
Video Resolution	Analog Port Maximum 1600x1200@75Hz.
Ethernet Port	
Number	1
Connectors	RJ45
Analog Port	
Number	1
Type	PS/2 and VGA
Connectors	PS/2 MiniDIN, 15 Pin D

Table 5: Technical Specifications

7.3 Minimum Requirements for Video Viewer and Virtual Media Interface

Successful operation of the video viewer and the remote client for virtual media requires the following minimum configuration on the client machine:

- 650 MHz Pentium or equivalent processor
- 128 MB of RAM
- 10 or 100BaseT NIC (100 recommended)
- xga video with graphics accelerator
- Desktop size setting of at least 800x600
- Color palette of at least 256 colors
- One of the following operating systems:
  - Windows XP Home or Professional Edition, Server Pack 2
  - Windows 2003 Server Standard Enterprise or Web Edition, Service Pack 1
  - Red Hat Enterprise Linux 4 (RHEL4) WS, ES, AS
  - SuSE Linux Enterprise Server 9 (SLES9)
- Internet Explorer 6.0 SP1 or later web browser (Windows operating systems only)
- Java JRE version 1.4.2 or later

7.4 OSCAR Interface Refresh Rates

The OSCAR interface synchronizes to the following refresh rates.

Resolution	Refresh Rate	Horizontal Frequency
640 x 480	60 Hz	31.5 Khz
640 x 480	72 Hz	37.9 Khz
640 x 480	75 Hz	37.5 Khz
640 x 480	85 Hz	43.3 Khz
800 x 600	60 Hz	37.9 Khz
800 x 600	72 Hz	48.1 Khz
800 x 600	75 Hz	46.9 Khz
800 x 600	85 Hz	53.7 Khz
1024 x 768	60 Hz	48.4 Khz
1024 x 768	72 Hz	56.5 Khz
1024 x 768	75 Hz	60.0 Khz
1024 x 768	85 Hz	68.7 Khz
1152 x 864	75 Hz	67.5 Khz
1280 x 768	60 Hz	60.0 Khz
1280 x 768	85 Hz	85.9 Khz
1280 x 1024	60 Hz	64.0 Khz
1280 x 1024	75 Hz	80.0 Khz
1280 x 1024	85 Hz	91.1 Khz
1600 x 1200	60 Hz	75.0 Khz
1600 x 1200	70 Hz	87.0 Khz
1600 x 1200	75 Hz	93.8 Khz
1600 x 1200	85 Hz	106.3 Khz

Table 6: Refresh Rates

7.5 Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Fujitsu Siemens product. If an issue should develop, follow the steps below for the fastest possible service: Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined. Check our web site at http://www.fujitsu-siemens.com/support and click on *Services & Support*. Click *helpdesk* on the left side of the page for a listing of technical support phone numbers in your area.

7.5.1 Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Go to the Fujitsu Siemens support Web site at http://www.fujitsu-siemens.com/support/ to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that Fujitsu Siemens provides in the online help or in the documentation that is provided with your Fujitsu Siemens product. If you suspect a software problem, see the documentation for the operating system or program.

590-771-501A

Information on this document

On April 1, 2009, Fujitsu became the sole owner of Fujitsu Siemens Computers. This new subsidiary of Fujitsu has been renamed Fujitsu Technology Solutions.

This document from the document archive refers to a product version which was released a considerable time ago or which is no longer marketed.

Please note that all company references and copyrights in this document have been legally transferred to Fujitsu Technology Solutions.

Contact and support addresses will now be offered by Fujitsu Technology Solutions and have the format *...@ts.fujitsu.com*.

The Internet pages of Fujitsu Technology Solutions are available at *http://ts.fujitsu.com/*...
and the user documentation at *http://manuals.ts.fujitsu.com*.

Copyright Fujitsu Technology Solutions, 2009

Hinweise zum vorliegenden Dokument

Zum 1. April 2009 ist Fujitsu Siemens Computers in den alleinigen Besitz von Fujitsu übergegangen. Diese neue Tochtergesellschaft von Fujitsu trägt seitdem den Namen Fujitsu Technology Solutions.

Das vorliegende Dokument aus dem Dokumentenarchiv bezieht sich auf eine bereits vor längerer Zeit freigegebene oder nicht mehr im Vertrieb befindliche Produktversion.

Bitte beachten Sie, dass alle Firmenbezüge und Copyrights im vorliegenden Dokument rechtlich auf Fujitsu Technology Solutions übergegangen sind.

Kontakt- und Supportadressen werden nun von Fujitsu Technology Solutions angeboten und haben die Form *...@ts.fujitsu.com*.

Die Internetseiten von Fujitsu Technology Solutions finden Sie unter *http://de.ts.fujitsu.com/*..., und unter *http://manuals.ts.fujitsu.com* finden Sie die Benutzerdokumentation.

Copyright Fujitsu Technology Solutions, 2009